



*Liberté • Égalité • Fraternité*  
**RÉPUBLIQUE FRANÇAISE**

FRENCH MINISTRY OF CULTURE

--

HIGHER COUNCIL ON LITERARY AND ARTISTIC PROPERTY

NATIONAL CENTRE FOR CINEMA AND THE MOVING IMAGE

HIGH AUTHORITY FOR THE DISSEMINATION OF WORKS AND THE PROTECTION OF RIGHTS ON THE INTERNET

## **MISSION REPORT**

# **Towards more effectiveness of copyright law on online content sharing platforms : overview of content recognition tools and possible ways forward**

Mission Chair: Jean-Philippe Mochon

Rapporteur for the CSPLA: Sylvain Humbert

Experts for HADOPI: Carla Menaldi and Didier Wang

Coordinated by Pauline Blassel

For the CNC: Laetitia Facon

*Report submitted to the CSPLA on 28 November 2019*

*The content of this document is binding only on its authors*

29 January 2020



## Summary

The protection of intellectual property rights on online sharing platforms today requires digital tools suited to their realities.

The most widespread, developed and effective solution for identifying protected content is known as *fingerprinting*, based on the conception that data have a unique digital identifier, analogous to human fingerprints. It is widely applied to audio and video content, in particular by YouTube, Facebook and Dailymotion. In this mission, several recognition algorithms were tested for robustness: based on these tests, the said robustness proved to be excellent, unless users accept particularly deteriorated content. Whether on audio or video content, fingerprint identification using currently available tools overlooks only a very small amount of content (false negatives) and misidentifies (false positives) an equally small number.

Undeniably mature and operational, the technique known as fingerprinting draws on a range of varied and competing solutions, implemented in a diversified manner. In some cases, for instance, platforms have integrated tools which they developed themselves, while in others, they have implemented that of a service provider. This wide range of solutions may appear to be a constraint for rightholders, forced to adapt to the tools specific to each platform to protect their content. The implementation of shared management solutions such as the one-stop shop developed by the French Association for the Fight against Audiovisual Piracy (ALPA) or solutions offered by providers specialised in offering content protection services on multiple platforms simultaneously are some of the operational responses to this diversity in fingerprints.

Fingerprinting creates a challenge for rightholders and platforms alike, as both groups must be able to sustain a reference base broad enough to enable content recognition, in a context where the flow of content uploaded is considerable. Both extensive storage capacity and rapid content analysis capabilities are required for a prompt and accurate response.

The digital fingerprint makes it possible to both block and monetise content on platforms depending on the rightholders' preference. The roll-out of the digital fingerprint has been supplemented by the implementation of a management interface with a variety of functionalities some of which can even be adjusted by users, as is the case with YouTube's Content ID. These interfaces, also referred to as CMS (*Content Management Systems*) offer rightholders the ability to ensure their rights are upheld, with varying degrees of sharpness and practicality, the two key characteristics distinguishing the tools currently on the market. When determining the quality of a solution, the list of functionalities offered matters as much as do the robustness and sharpness of the recognition tools.

Of central importance on the main platforms, the use of the digital identifier (so-called *fingerprinting*) appears to be the standard today, but should not overshadow the existence of other techniques, which may be complementary, even if they do not offer the same efficiency and usage options. For instance, *hashing*, the use of metadata and *watermarking* (a form of "digital tattoo") are all considered alternative methods, but cannot compete in every way with digital fingerprinting.

While the developments ahead for recognition tools are still uncertain, artificial intelligence is likely the most promising avenue to date, with the *caveat*, however, that it should not be considered a replacement for the fingerprinting technique, but a further tool expected to contribute to improving the sharpness of recognition tools. Other methods, based in particular on image analysis, could also be envisioned, insofar as they are based on available or developing technologies, but raise other issues, for instance as pertains to privacy, and in so doing, highlight the advantages of the fingerprinting technique to date.

Platforms, rightholders and users have diverging perceptions and expectations regarding the development of content recognition tools.

Only certain platforms, under heavy pressure from certain rightholders, have actually implemented content recognition tools based on digital fingerprinting and have signed licensing agreements with music producers. The platforms which, despite the service offers available on the market, have not yet implemented such tools, are showing their resistance to upgrading, while their counterparts have both paved the way and are seen the standard by rightholders.

As to the rightholders, their situations are very different and contrasting. The first difference lies in their attitude towards the presence of their content on the platforms. In light of the economics of their sectors, producers of audiovisual and musical works see platform-based sharing, either as a risk to their main modes of commercialisation more than anything else (this is the case with audiovisual), or first and foremost as an essential means for spreading their content (as in the music industry). This distinction explains why they predominantly choose to block sharing in the former case and seek monetisation in the latter.

While rightholders in cinema and music have operational solutions at their disposal on the platforms, the rightholders in other creative sectors must find a way to cope, despite the absence of any technological recognition solution implemented on the sharing platforms, which have thus far done no more than invoke the application of the host status. Some rightholders in the visual arts, and in particular those of photography, have set out to establish reference bases and technological tools capable of identifying their works found on platforms, and thus giving them the opportunity to implement any licensing agreements they may have signed. In other sectors (written media, “graphic music”, video games), it is no more frequent to see recognition tools deployed by sharing platforms, as the rightholders voice expectations of very differing degrees in this regard.

As to users, it would appear, based on the surveys commissioned by Hadopi, that a relatively large number of them have experienced content blocking during an upload, but by and large understand the reasons for this blocking, thus demonstrating a certain familiarity with the principle of intellectual property rules. It is important to distinguish between such users and so-called “*YouTubers*”, user-videographers, who are unique in that they gain income from the content they produce. Their expectations where recognition tools are concerned fall in step with a general demand for transparency in rules and recognition of their creative contribution. They focus in particular on the effective benefit of exceptions to copyright, as well as, in contrast, access to tools enabling the

protection of their own content, and lastly, the rules that apply when they wish to challenge a claim made by a rightholder.

Against this motley backdrop, in which players with a wealth of experience in fingerprinting tools are flanked by vast sectors that remain outside the scope of content recognition, Article 17 of the Directive on Copyright in the Digital Single Market is reshuffling the deck by clarifying the legal framework. This framework is expected to enable a shift towards the effective application of copyright on online content-sharing platforms, which are now clearly considered to be carrying out an act of communication to the public by making shared content available to it.

Recognition tools will enable the platforms to make their best possible efforts to block and remove unauthorised content, the condition for their absence of liability. While Article 17 of the Directive itself does not make any particular technology mandatory, it refers, in defining these best efforts, to the *“high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information”*. In this sense, it defines an approach that is concurrently rigorous, pragmatic and scalable.

In the field of audio and video, which are already covered by fingerprinting systems, it is now essential that concerned parties make reference to the latter in order to qualify as having made their best efforts, while the relevant and necessary information is to be assessed according to the nature of the rights (copy of protected content, fingerprints, metadata). All sharing platforms covered by the Directive will, in this sense, have to make an effort to upgrade, a process now fully feasible, given the wide range of solutions available on the market. In the other sectors, defining the best efforts of the platforms and the relevant and necessary information to provide is more of a blank slate approach, considering the platforms’ current practices, and will require both consultation and expertise.

For platforms covered by Article 17, the deployment of recognition tools can therefore no longer be limited to a form of response, depending on how interests and balances of power converge, to requests from specific categories of rightholders. It must proceed from a global approach to the protection of copyright and related rights, which must be open to the rightholders in the various sectors, who must provide the platform with the necessary and relevant information for it to perform the due diligence for which it is responsible.

This new legal framework also implies new guarantees of transparency for rightholders on the way in which their works and other protected subject matter are used for profit. This transparency should apply both to situations in which unauthorised content is blocked and removed, and to the exploitation of content in the case of the agreements authorising it. It contributes to a general shift towards greater transparency in the operation of tools deployed on platforms, also provided for by the Directive, to the benefit of users.

Lastly, the implementation of Article 17 is also an invitation to define the balances that will govern the application of copyright on online content-sharing platforms. Article 17 provides for the continued validity of existing exceptions when it comes to short quotes and parodies, caricatures and pastiches. This concern must be addressed through the implementation of an effective mechanism for settling

complaints and disputes, which the Directive surrounds with new guarantees connected with existing practices, in particular by providing for a human review of removal and blocking disputes, and the involvement of an impartial dispute settlement mechanism. It could also be beneficial taken into account, on a voluntary basis, in defining the management rules associated with the content.

On all the complex issues which the existing and future recognition tools require, the implementation of Article 17, with the dialogue and guidance role entrusted by the Directive to the European Commission, will play an important part. In addition, a number of important subjects would make it worthwhile for the Member States to conduct a consultation, or even define a regulation. A sustained dynamic in this regard will make possible the effective application of copyright on sharing platforms.

# Table of Contents

Introduction.....	10
1. - State of the art of content recognition technologies and their deployment.....	12
1.1. - By describing and assessing the robustness of existing recognition technologies, the mission was able to reveal the central place of fingerprint-based systems. ....	12
1.1.1. - A state of the art now centred on digital fingerprinting systems for audio and video content. ....	12
1.1.2. - Other supplementary methods with more limited effectiveness.....	26
1.2. – The practicality and the sharpness of fingerprint content recognition technologies can be assessed by analysing their implementation. ....	31
1.2.1. - While recognition tools are already extensively used, deployment still varies depending on the players and sectors. ....	31
1.2.2. - There exist several ways of organising tools that go beyond the models developed internally by some platforms for their own use.....	34
1.2.3. - A closer look at the detailed functioning of the tools with regard to their practicality and sharpness.....	41
1.3. - Current avenues for development do not call into question the central role of fingerprint-based technologies. ....	49
1.3.1. - Artificial intelligence and content protection. ....	49
1.3.2. - Content analysis solutions used today for purposes other than copyright protection. ...	52
1.3.3. - Longer-term avenues for development .....	57
2. - Stakeholder perceptions and expectations: content recognition tools at the crossroads of the visions and interests of platforms, rightholders and users.....	59
2.1. – Thus far, the platforms have focused on becoming proficient in deploying content recognition tools, regarding both their concepts and their scope and methods of implementation. ....	59
2.1.1. - Audio and video sharing platforms: content recognition was first deployed on a large scale by YouTube, which determined its functionalities and uses.....	60
2.1.2. - Generalist social media and other platforms have been able to deploy audio and video content recognition tools. ....	64
2.1.3. – The quest to control costs associated with content recognition for platforms and market responses.....	66
2.2. – Rightholders: the wide range of expectations when it comes to recognition tools echoes the diversity of their situations with respect to sharing platforms. ....	68
2.2.1. - Film and audio-visual producers and distributors favour the blocking function to preserve the economic value of their rights.....	68

2.2.2. - The main television channels have come to make intensive use of content recognition tools. .....	72
2.2.3. - The vast majority of music rightholders have licensing and monetisation aims.....	74
2.2.4. - Rightholders in other sectors do not have recognition tools deployed on the platforms.	75
2.2.5. - The expectations of rightholders with respect to content recognition tools are thus varied, reflecting the differences in practice, depending on the sectors and the size of the actors.....	79
2.3. – Users perception: widely-varying experiences on the ground, acceptance of copyright rules in principle, and implications with regard to the availability of content.....	80
2.3.1. - Presentation of the quantitative study methodology.....	80
2.3.2. - Massive use of the social media, with varying degrees of user involvement.....	81
2.3.3. While Internet users have a good understanding of the implications of copyright rules as applicable to content sharing platforms, their knowledge is more relative when it comes to the rules on exceptions. ....	83
2.3.4. - Many users have experienced blocking of their content on social media or platforms, and generally understand the reasons behind it. ....	86
2.3.5. – Blocking instances related more to video content, are generally well understood and often uncontested, but users underline fear, complexity and even uselessness as reason not to contest. .....	90
2.3.6. - Initially treated by platforms like any other users, though they also tend to be seen as rightholders, videographers remain in an ambivalent position with regard to recognition tools..	98
3. - Article 17 of the Directive on Copyright in the Digital Single Market makes content recognition tools central to the new balance still to be built. ....	101
3.1. Content recognition tools are an essential aspect of the implementation of Article 17, which requires actors to come up to standard in this respect.....	103
3.1.1. - The blocking and removal procedures provided for in Article 17 will be based on the implementation of content recognition tools, at least for audio and video content. ....	104
3.1.2. - For content authorised by rightholders, tools will also be needed to identify acts of exploitation .....	106
3.1.3. - As a result, platforms will need to make efforts to ensure they are up to standard on the protection of rights.....	107
3.2. The approach adopted for the Directive makes it possible to address many of the concerns raised during its discussion. ....	109
3.2.1. The approach adopted for the Directive is based on a pragmatic and proportionate implementation of recognition tools. ....	109
3.2.2. - Article 17 provides a new legal framework for content recognition tools, the practical importance of which was, until now, equalled only by the lack of transparency.....	110



3.2.3. - Article 17 by no means sets the stage for a single dominant player and instead lends itself to a variety of models in its implementation. ....	112
3.3. - Article 17 calls for the definition of a concerted and differentiated approach when it comes to content other than fingerprintable audio and video. ....	115
3.3.1. – Photography and Visual arts. ....	115
3.3.2. - Written works in the field of press and books. ....	117
3.3.3. - Rights of music authors, composers and publishers. ....	118
3.3.4. - Audiovisual Authors’ rights. ....	119
3.3.5. – Music rights pertaining to “commercial use of music in graphic form”. ....	120
3.3.6. - Rights of video game publishers. ....	120
3.4. - Content recognition tools will be central to the new balance between the parties interested in sharing protected content. ....	121
3.4.1. - For users: recognition tools, constraints and freedoms. ....	121
3.4.2. - The case of professional or semi-professional users: towards an increasingly organised dialogue with the rightholders of shared content. ....	127
3.4.3. - Between rightholders of shared works: Article 17 will lead to greater formalisation of the rules applicable in the event of conflicts of rights or rules. ....	129
3.4.4. - The definition of these new balances requires a dialogue and shared guidelines, with a major role for the European Commission. ....	130
Conclusion .....	133
Appendices .....	135
1 - Mission letter .....	135
2. - Characteristics of content recognition tools .....	137
3. - Further details on technology robustness assessments .....	140
4. - Matrix of usages observed .....	143
5. - Provisional and forward-looking information on the possible content of the concepts of “best efforts” and “relevant and necessary information” .....	144
6. - List of persons heard .....	146

# Introduction

Scope of the host status, effectiveness of copyright, filtering and blocking, etc.: those few words are enough to describe the debate generated by Article 13, now Article 17, the most heated of all those that emerged before the adoption in spring 2019 of what is Europe's most significant copyright reform in two decades. Beyond the catchwords "#Yes2Copyright" and "#SaveYourInternet", the content recognition tools already in use on sharing platforms, their usefulness, limits, or even dangers -- and in any case their future -- were thus at the heart of the discussion around the Directive on Copyright in the Digital Single Market<sup>1</sup>.

These recognition tools, the most widely used of which is the Content ID algorithm, which YouTube uses to verify the 500 hours of new video which its users share every minute, were far from being ready to play the leading roles in public debate. Established on video-sharing platforms and other social media to limit the presence of unauthorised content, they remain little-known. And yet they affect the day-to-day practices of millions of users and determine the reality of the rights of entire sectors of creation. Imposed on users, and hardly the subject of much more negotiation with rightholders, they came into the public eye for the first time during the debate on the draft Directive, where their core concept and procedures were at the focus of heated debates. However, the massive information asymmetries on the subject, between platforms, users and rightholders, were such that no composed discussion was really possible.

It is in this context that the present mission was carried out, in a joint effort uniting the CSPLA, HADOPI and CNC for more than six months, immediately upon the Directive's adoption, and parallel to the Government's preparations to transpose the Directive. The issues at stake when it comes to recognition tools had already been well described, during the Directive's negotiation, by an initial mission of the CSPLA, led by Olivier Japiot until November 2017<sup>2</sup>. Extending from this work, this mission was able to look to the future, on the basis of the European text adopted. By bringing together the legal, economic and technical expertise of the three institutions, it aspires to build an overview of players' practices and expectations, and to chart out the first ways forward in implementing the Article 17, of which the French authorities have been ardent supporters.

After nearly sixty hearings, and meetings with more than one hundred prominent experts from France, Europe and the world, the mission first offers an overview of players' practices and the technologies deployed, as well as an assessment of their performance. From this panorama view, supported by in-depth tests, it emerges that: fingerprint recognition algorithms have reached a real level of efficiency in recognising content on sharing platforms; the risks of over-blocking can be overcome by appropriate

---

<sup>1</sup> Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and related rights in the digital single market.

<sup>2</sup> See the report of the CSPLA Mission on automatic content recognition tools for works on online platforms, drafted by Mr Olivier Japiot, Chairman of the Mission, and Mrs Laure Durand-Viel, rapporteur: <https://www.culture.gouv.fr/Sites-thematiques/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-propriete-litteraire-et-artistique/Travaux/Missions/Mission-du-CSPLA-sur-les-outils-de-reconnaissance-des-oeuvres-sur-les-plateformes-en-ligne>.

practices; and lastly, in sectors other than audio and video, their absence is impeding effectiveness of rights.

Moving beyond this observation, the mission focused on mapping actors' expectations. Based on the interviews it conducted, as well as on detailed quantitative and qualitative opinion studies, it was able to better identify the determinants behind the perspectives of sharing platforms, rightholders and users. From this, it notes that Article 17 of the Directive came at a time when the *de facto* mode of regulation used up to then, determined by platform discretionary decisions, was reaching its limits. The platforms' smooth operation, the effectiveness of intellectual property rights protection and the transparency of decisions for users are imperatives that can be shared, but that can no longer be guaranteed by unilateral technical decisions alone. In this sense, Article 17 came at just the right time.

Lastly, the mission team set out the first steps towards the ambitious and concerted implementation of Article 17. Taking into account the lessons described above and the analysis of the Directive's text, it concluded that digital fingerprinting tools are naturally destined to play a central part in the recognition of audio and video content, which should significantly improve the protection of rights by bringing operators up to speed. For all other protected content covered by Article 17, in particular written and image content, concerted choices must be made to define the due diligence expected of platforms, based on the information to be provided by rightholders for the protection of their works. The flexibility inherent in the "best efforts" mechanism provided for in the Directive, always dependent on the state of the art and the information provided by rightholders, will enable it to be implemented in a pragmatic manner. To this end, a multitude of technological solutions and commercial offers are already emerging, and are expected to enable all the platforms to meet the due diligence requirements set out by the Directive.

Far from threatening freedoms or the protection of privacy, the Directive can be an opportunity for shared progress, expected from the application of copyright on sharing platforms. By regulating practices and organising impartial settlement of disputes, it promotes the proper use of recognition tools. From technical auxiliaries put to work for contractual relations hitherto covered by business secrecy, these tools are turning into controlled parameters of the new balances in copyright. This transformation is an issue of capital importance for the future of copyright in the digital age. Beyond the transposition of the Directive in each Member State, it calls for dynamic and concerted regulation, the next stage of which is the exercise of dialogue and, at a later stage, guidance entrusted by the Directive to the European Commission.

# 1. - State of the art of content recognition technologies and their deployment.

The recognition of content protected by intellectual property rights by online content-sharing service providers points to a state of the art that today focuses on digital fingerprinting systems, although the concurrent use of other methods can be considered a complement.

Sharing platforms have deployed content recognition tools to protect and enhance these rights on a large scale, mainly through the use of fingerprinting systems. However, the situation still varies depending on the actors and sectors, and relates to several organisational methods.

The evaluation of these tools involves reviewing their operating mode for their robustness, their practicality and the sharpness of their analysis in order to establish an analysis and comparison grid.

## 1.1. - By describing and assessing the robustness of existing recognition technologies, the mission was able to reveal the central place of fingerprint-based systems.

### 1.1.1. - A state of the art now centred on digital fingerprinting systems for audio and video content.

#### 1.1.1.1. - *General operating principles and existing methods for evaluating the robustness of fingerprinting systems.*

##### ➤ Description of fingerprint systems

The digital fingerprint content recognition technique, commonly known as *fingerprinting*, consists of generating, then using a unique digital representation of content which then constitutes a fingerprint of the latter, distinct from the work itself.

The technologies used to generate these fingerprints reduce or simplify entire content units – image, sound, video, text, etc. – picking out only their characteristic components. This process is not reversible. Therefore, the original content in its entirety cannot be recreated from the fingerprint.

Rather than directly assessing the similarity between two documents (between two images, two sound tracks, or two texts), these tools establish their similarity by comparing their fingerprints. It is hypothesised that the similarity of two documents is proportional to the similarity of their fingerprints. The similarity is thus established by creating a fingerprint for each document and the metric used to compare these fingerprints. A content recognition system thus mainly draws on the comparison of these fingerprints.

Fingerprints are easier to handle than the documents themselves. They are often lighter (a few hundred bytes for the fingerprint of an image versus several million bytes for the image itself) but also more robust (invariable to small changes to the content).

Content recognition systems are generally composed of a reference base in which the fingerprints of all the documents to be identified are stored. For this purpose, a very specific algorithm is applied to each document by generating a fingerprint, which is then placed in the database. Generating the fingerprints of millions of photos, thousands of hours of video, and vast sound archives is very demanding in terms of computing and storage resources.

Once this database is created, the system is used as a search engine. To find out whether an unknown document is found in the reference base, the relevant fingerprint must be excerpted, then compared with the fingerprints pre-calculated and stored in the base. This comparison then makes it possible to determine whether similar documents have been found.

This architecture, which is common to systems for searching for similar content, invites several comments. It is by comparing fingerprints that one can judge whether two documents are similar or different. Obviously, the nature of these fingerprints has a fundamental impact on the establishment of similarity. Texts cannot be compared in the same way as images are, and images of faces cannot be compared in the same way as images of landscapes are. It is the fingerprints that form the foundation for establishing similarity.

One or more matches can appear between the fingerprint of a document to be identified and the fingerprint of an unknown document. Beyond a certain threshold of similarity, it can be deemed that the two documents under review are indeed similar.

However, it should be stated that mismatches also occur, referred to as false positives. The system may find unintended similarities, without any real foundation from the perspective of us humans, but which deceive the system. Often, supplementary (and generally very expensive) processing tools must be brought in to filter out these false positives, thus reducing false alerts and reporting only founded cases. Fingerprints should therefore be designed as far as possible to limit false positives, with the provision that it is impossible to eliminate them completely, but also to avoid false negatives, i.e. failure to match up two documents when these are in reality similar.

To conclude, there is no universal, relevant fingerprint, whatever the recognition task. A fingerprint is specialised and addresses a specific application task, in a limited field (visual, sound, textual).

In order for recognition tools to be effective, the reference base must be dynamically augmented with new fingerprints related to the documents to be identified, something which not all existing systems are necessarily able to do. Some systems are able to accommodate steady database enlargement over time; others require a restart after a complete regeneration of the database increased by new content; still others are completely static and are only able to take into account new content by multiplying the databases they manage.

The reference base is used to identify works over several years, thus raising the question of the evolution of fingerprinting techniques. If a new version of a fingerprint proves to be better than the

one currently used, is the fingerprints' (retro)compatibility guaranteed? This is not always possible and, in this case, is hampered by the problem of how to access the original documents again to generate new fingerprints replacing those pre-calculated. This generation process can be very difficult, due to the volume of documents to be reprocessed, the calculation and storage resources needed, or quite simply because the original documents are difficult to access.

In summary, a content recognition system based on fingerprints requires having access to an algorithm that calculates the fingerprint of each document to be identified, a database where all fingerprints of the corpus of interest are stored, and a search engine that determines whether there are similar fingerprints in the database to that of the unknown document to be tested.

### ➤ Robustness tests: methodology, criteria

The mission's aim was to evaluate the recognition tools, first and foremost the tools based on the fingerprinting technique.

The way in which robustness tests are conducted is informed by the academic research listed below and by the work of professional organisations<sup>3</sup>.

To assess the robustness of a technology as a whole, indicators are generally used to observe the precision of the detection, its recall, its response time, its memory consumption or its computing resource requirements, as well as other often sophisticated metrics intended to characterise certain specific performance levels<sup>4</sup>. Assessments are usually specialised by broad task.

---

<sup>3</sup> The mission would like to thank IFPI and Movielabs for having provided information about their work on the subject.

<sup>4</sup> In general, these measures require a carefully determined set of questions on the one hand, and relevant answers to these questions on the other, for a given corpus. The term often used is "ground truth". The main measures are recall, i.e. the proportion of relevant documents returned by the system out of all the relevant documents, and precision, meaning the proportion of relevant documents out of all documents returned by the system.

### Indicators used to measure the performance of recognition technologies

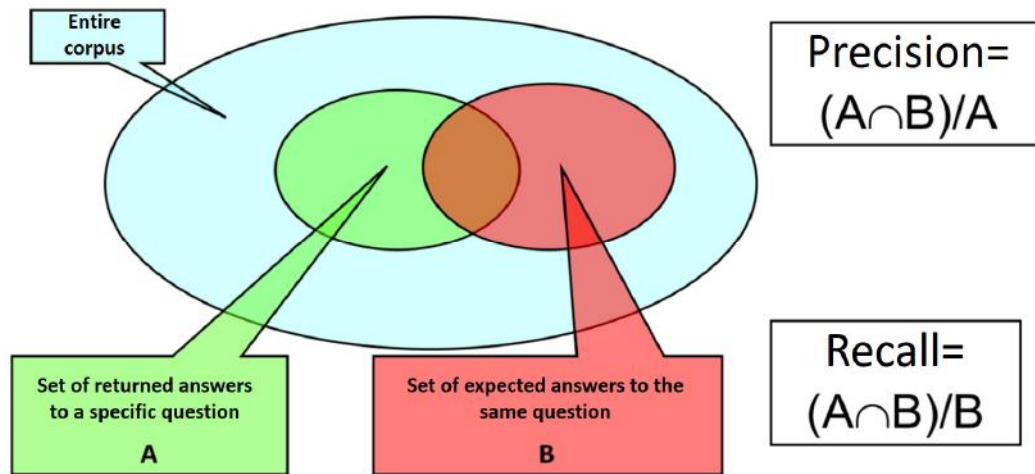


Figure 1

An illustration of the two most commonly used indicators when conducting search engine performance measurements. A set of questions is developed, to which the responses are known exactly.

As an example, all the videos in possessed by the National Audiovisual Institute (Ina) in which the CSPLA is mentioned are manually and very accurately identified. These videos form set B, which we will use further on. The entire Ina video library is then analysed using an automatic content recognition system. In the last step, the system is asked a specific question by running a search for content, based on a video excerpt that makes reference to the CSPLA.

The responses returned (set A) are compared with those expect to see returned (set B). The precision is defined by the number of items present in the intersection of A and B, over the number of elements of A.

If answer A contains 100 elements, but only 10 of them belong to B, then the degree of precision is 10%. Here, the system shows low precision. The 90 items in A are false positives. The system incorrectly flags them.

The recall is the number of items in this same intersection, divided by the number of expected responses. If B contained 20 items, then the recall would be 50%. The system found only half of what was expected.

Those missing are false negatives. The performance of several systems can be compared by observing their recalls and calculated precision on the same dataset, with the same questions, and the same expected answers. The comparison is thus reliable, reproducible and objective.

Source: Hadopi with CNRS-IRISA (L. Amsaleg)

Launched in the 1960s<sup>5</sup>, this experimental evaluation approach has been adopted by many scientific communities. Originally developed more for text, with the TREC assessment campaigns<sup>6</sup>, the approach was then used for several media. The works of Éric Gaussier, a professor at the Grenoble Computer

<sup>5</sup> See C. W. Cleverdon's investigation into the comparative efficiency of indexing systems: <http://sigir.org/resources/museum/>

<sup>6</sup> Text Retrieval Conference: <https://trec.nist.gov/>

Science Laboratory (LIG) give a good idea of these protocols, and more generally about what information search engines can do.

Each year, the MediaEval congress, specialising in the assessment of systems processing multimedia data, is convened to discuss these protocols tasks related to the recognition of multimedia content directly resulting from this work<sup>7</sup>. It presents test sets, measures to assess the quality of the results found, safeguards needed to avoid bias and poor interpretations, etc.

### 1.1.1.2. - *Identifying audio content.*

#### ➤ A range of existing solutions

Since the late 1990s, several dozen technical *fingerprinting* solutions for audio have emerged. However, not all of them survived. Regularly, waves of companies emerge in this area, only to fade out of the landscape just as quickly. Some technologies are wholly or partly in the public domain or based on academic work. These include the *open source* Panako and Acoustid solutions and the research carried out by the University of Indiana, the University of Ghent and IRCAM (Institute for Research and Acoustic/Music Coordination).

One of the most well-known and oldest commercial solutions is that produced by Audible Magic, founded in 1999, which states that its reference base now contains the fingerprints of around 25 million audio titles. Originally used for to automatically monitor songs or radio advertisements, these technologies quickly came into applications in the field of content protection, in the early 2000s, when large-scale analysis of a significant amount of content disseminated on the Internet was required.

YouTube has developed its own internal solution: Content ID. The fingerprint base of this multimedia solution, as it now covers audio and video content, contains more than 80 million references. More recently, YouTube has supplemented its system by creating a tool called Melody ID, specialised in automated melody identification<sup>8</sup>. Audible Magic is working on an equivalent technology<sup>9</sup>.

The companies Gracenote (with its MusicID technology), Kantar Media, Simbals, ACRcloud, SoundMouse, BMAT, Yacast and SoundHound have also developed their own audio fingerprint recognition solutions for various uses (audience measurement, monitoring of works broadcasted on radio, content protection, synchronisation of applications, digital archiving assistance, etc.).

The level of efficiency of these technologies may also vary significantly depending on the objectives sought: while the solution proposed by Audible Magic seeks above all to recognise recordings with a high level of certainty in order to avoid any false positives, those developed by Shazam or Echo Nest (Echoprint) are, on the contrary, much more flexible and tolerant (the aim of the latter is even, if they

---

<sup>7</sup> See: <http://www.multimediaeval.org/mediaeval2019/>

<sup>8</sup> Unlike traditional digital fingerprinting systems that recognise the specific recording of a song as performed by one artist in particular, the algorithm used by Melody ID is intended to be more flexible. Thus, it can identify a tune played, hummed or sung, even if the performer or arrangement are different from the original ones.

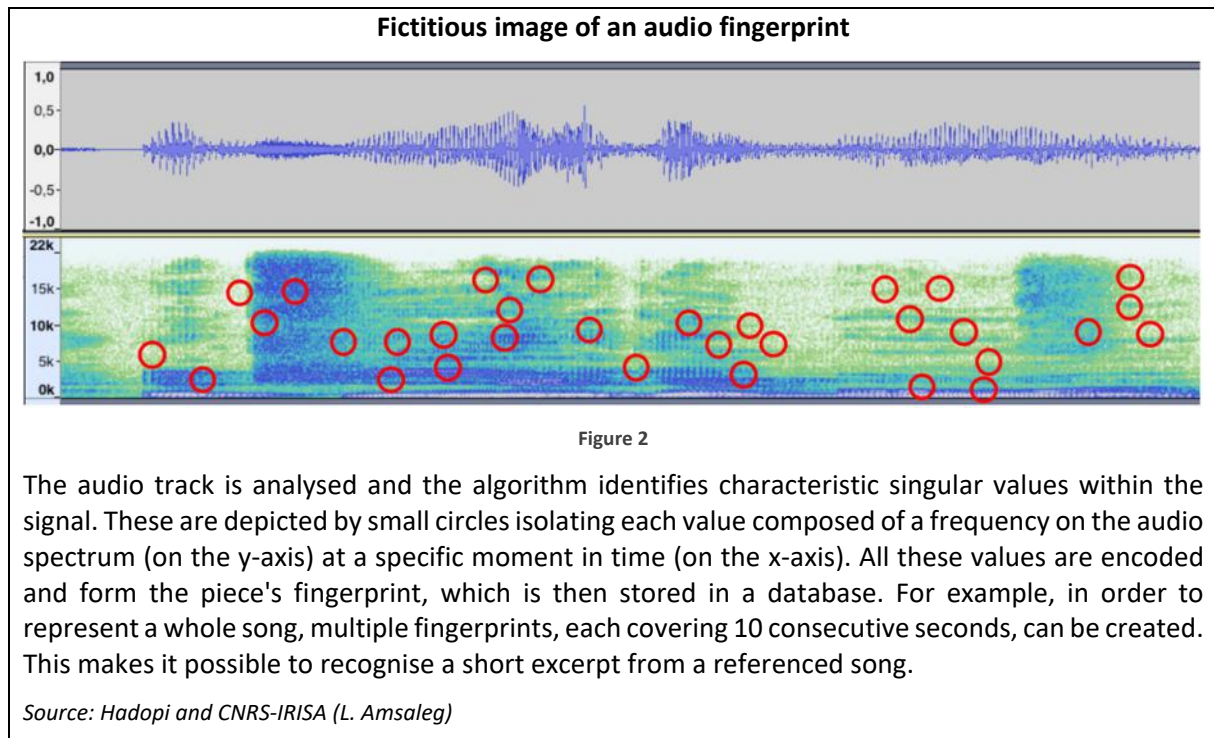
<sup>9</sup> These melody recognition tools – the performance of which is still being fine-tuned – are currently only available to a limited number of rightholders. The risk of false positives is high, especially when short samples are analysed.



have not recognised an audio excerpt analysed accurately, to suggest a piece of music that roughly resembles the excerpt in question).

### ➤ Operating principles

To generate digital fingerprints of audio works, existing systems rely on a variety of characteristics such as a piece's frequencies, key, rhythm or variations in sound. The fingerprint is a kind of equation of these sequences of characteristic components.



As only certain components of the work are taken into account, the file of an audio digital fingerprint is generally smaller in size than the file of the original content. However, the more accurate the technological solution and the shorter the detection interval, the more significant the size of the fingerprints.

### ➤ Robustness test results

The tests carried out by Hadopi as part of this mission show that the main technologies used by digital platforms have a strong overall ability to recognize musical excerpts, despite the addition of intentional distortions on relatively short excerpts, in the range of 20 to 30 seconds or even less in certain cases.

Deformations such as changes in key, deterioration of quality, addition of echoes, tremolos or reverberation, do not seem, in most of the cases tested, to prevent detection provided that these distortions are not taken to the extreme. Similarly, a piece of music embedded in the soundtrack of a film or recorded with a microphone during a public broadcast is correctly identified after a few seconds

(if it is the original piece and not a new arrangement), despite the presence of moderate voices or parasitic noise. The technologies used by social media and community platforms are generally more flexible in dealing with alterations in audio signals because users of these sharing services often upload content of average or deteriorated quality.

In contrast, detection is not always successful if the recording is a piece of music played in an enclosed space such as a disco, as the bass levels are significantly modified (“subwoofer” effect) and many bursts of voice disturb the sound. While a technology such as Shazam, which is deliberately flexible, can recognise a piece in such a context, this is not necessarily the case with some versions of Audible Magic's solution, which require a higher level of fidelity to establish with certainty the match with the original work. Similarly, mixes more commonly referred to as “*mash-ups*”<sup>10</sup> are not always detected when the fingerprint resulting from this mix is, for the technology, too distinct from each of the songs composing it.

A series of tests involving nearly twenty types of alterations (more than half of which were severe to the point of significantly deteriorating listening comfort – see details in Appendix 3 of this report) was subjected to several audio content recognition tools, developed internally by digital platforms or operating independently. The various solutions tested were all able to recognise the least altered excerpts automatically and without trouble.

Where the most deteriorated excerpts are concerned, including playing heavily on key and accelerating the speed of play, only one solution stood out in particular, automatically recognising the right piece of music in 94% of cases. The overall success rates of the other solutions were generally between 30% and 40% for this series of targeted tests, which seems consistent with the fact that one-third of the tests involved slight to moderate distortions and two-thirds severe distortions. Moreover, unsurprisingly, the most flexible solutions (in other words, those designed to recognise even low-quality recordings) scored better than solutions requiring a high level of fidelity to the original work to authenticate a match.

In conclusion, it is observed that the main content recognition technologies based on audio digital fingerprints can now easily identify good or medium quality excerpts of music. The main difference observed between the different solutions lies in the way trigger thresholds are set in these systems. If the threshold is too high for the required quality, some slightly deteriorated reproductions of content will not be recognised, as slight variations or interference are enough to disrupt the content recognition tool.

Conversely, if the threshold is too low as regards the quality required, a risk of over-detection will result, for example if two musical excerpts are accidentally similar. Similarly, the risk of false positives increases when the threshold on listening time decreases: it can happen that several distinct pieces of music contain very short sound passages that are similar or even identical, particularly in the case of electronic or classical music.

---

<sup>10</sup> Mixing two or more titles into one.

### 1.1.1.3. - *Identifying video content.*

#### ➤ A multiplicity of existing solutions

The National Audiovisual Institute (Ina) is seen as a pioneer in digital fingerprint-based content recognition technology, with its tool known as “INA-Signature”, used internally from as early as 2006 to monitor the dissemination and reuse of its archives.

Already in 2007, the platform YouTube developed its own video content recognition technology, first called “Video Identification” and later “Content ID”. Today, this technology operates concurrently on an audio fingerprint database and a video fingerprint database. More recently, Facebook also elaborated its own solution based on image and video fingerprinting, as well as audio fingerprinting, integrated into its Rights Manager tool.

A number of service providers specialised in content protection have also developed their own video recognition technology based on digital fingerprinting in order to address internal and operational needs, or to provide an offer independent of the technologies developed internally by the platforms. Examples include Vobile (with its VDNA solution), Audible Magic (which also offers a solution dedicated to video), Videntifier, Civolution, Friend MTS, TMG and PEX.

Consequently, whether for audio or video, a range of technical solutions providers operate on the market, to the extent that in audiovisual content, the audio and video fingerprints are not always interlinked.

#### ➤ Operating principles

The operating principles of digital fingerprint-based content recognition systems for video are quite similar to those used in audio. As with audio, content recognition is a two-step process: first, a fingerprint of the analysed video must be generated; then, the reference base is searched to determine whether the fingerprint matches that of a known work, whether fully or partially.

The difference lies in the nature of the fingerprint and the method used to analyse it.

As to the size of the fingerprints compared to the size of the original content, it should be noted that the more points and analysis criteria there are, the “heavier” the video content's fingerprint will be and thus the more IT resources will be needed to perform recognition.

In the case of videos (animated images), the characteristic elements on which fingerprints are based may be varied in nature. Some technologies focus on the local motion areas (i.e., from image to image, which parts are in motion and which parts remain immobile). Other solutions can measure the levels of colour or contrast found in the image and track how they develop over time. Another technique consists of recognising specific still images taken from the video signal (see 1.1.1.4.). Analysing the frequency of view changes during a video is yet another a technique that can highlight characteristic components: the likelihood of having multiple audiovisual segments edited at strictly the same pace – over a given duration and down to one-tenth of a second – is very low.

The technologies in this area have advanced considerably over the years. Once upon a time, it was enough to darken the corners of a video and superimpose a grid of small repetitive patterns (a simple procedure, albeit not within the reach of every Internet user) to buck the system. These simple workarounds are no longer effective, and the recognition systems have been adjusted to take them into account. Still, some users continue to take play with these technologies' limitations.

Similarly, thresholds on detection duration have seen a downward trend, and some technologies can now recognise video clips lasting a few seconds.

The most dynamic fingerprint recognition systems can also be applied to events broadcast live. This capability appeals primarily to sports leagues. In practice, the fingerprint of a sports competition broadcast is made as close as possible to the OB truck responsible for producing the audiovisual programme. The video fingerprint is generated in short segments throughout the match and the segments are added immediately to the reference base of the relevant fingerprinting system. By dint of the sheer speed involved, the fingerprint is thus placed in the database several tens of seconds or even a few minutes before unlawful rebroadcasts take place, based on the current lag times in "traditional" terrestrial or digital broadcasting.

#### ➤ Robustness test results

On the basis of the targeted tests carried out by Hadopi for the purposes of the mission, it can be concluded that the main content recognition systems in use today do make it possible to correctly identify works for which reference fingerprints have previously been made (see Appendix 3 of this report for details on the methodology used).

Four sets of tests were carried out on a range of popular platforms that had developed their own content recognition tools or used third-party technologies. The excerpts tested, ranging in length from a few minutes to more than 15 minutes, included works of fiction, cartoons, documentaries and television programmes which themselves included clips from films or music videos. In total, more than 150 excerpts amounting to nearly 20 hours of videos were posted online, with the consent and cooperation of the rightholders concerned.

Through a first series of tests, referred to as basic tests, the minimum expected detection capabilities were verified. The various solutions evaluated all proved to be effective in 100% of the cases used in these basic tests, consisting of excerpts posted on sharing platforms, i.e. passages directly taken from the original works, without having first undergone any specific transformations or processing.

A second more extensive set of tests assessed the ability of the tools to recognise video clips modified using traditional, moderate effects. The effects applied were those customarily seen on digital platforms when users try to deceive recognition tools, namely, deterioration of image quality, acceleration or reduction of playback speed, enlargement or reduction of image size, rotation effects or, for instance, fixed or moving distortions to images. Applying these effects can already significantly impact users' viewing experience.

### Screenshots from the second set of tests, with moderate alterations

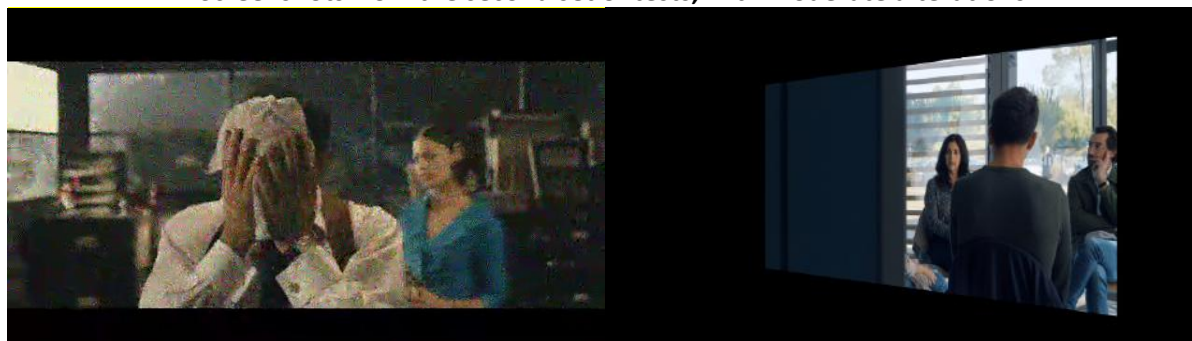


Figure 3

Examples of moderate alterations (quality deterioration on the left and distorted perspective on the right).

Source: *Hadopi*, with the permission of Gaumont and TF1.

The tools were able to easily recognise 80% to 100% of the content tested. In those cases where the works were not accurately identified, significant geometric deformations or juxtaposition of several videos side by side were tested. In rare cases, the failures were related to standard effects such as a 180° rotation of the image or a slowing or acceleration of the playback speed by more than 25% compared to the original speed.

In a third series of tests, the ability of the tools to recognise very markedly modified video clips or those with several distinct effects was assessed. Examples include a doubling of the playback speed, marked changes in hue, image jitter effects, as well as video editing (splitting an excerpt into small sequences in disorder) or the accumulation of zoom and rotation effects or regular colour variations and image magnification during playback. When modified in this manner, excerpts posted online can no longer be easily viewed by users, as some of the effects prove particularly disturbing. For example, part of the action takes place off screen, some details become invisible, etc. Considering these changes and the degraded appearance of the image, watching the video is an effort that is difficult to sustain over time.

### Screenshots from the third set of tests, with severe alterations



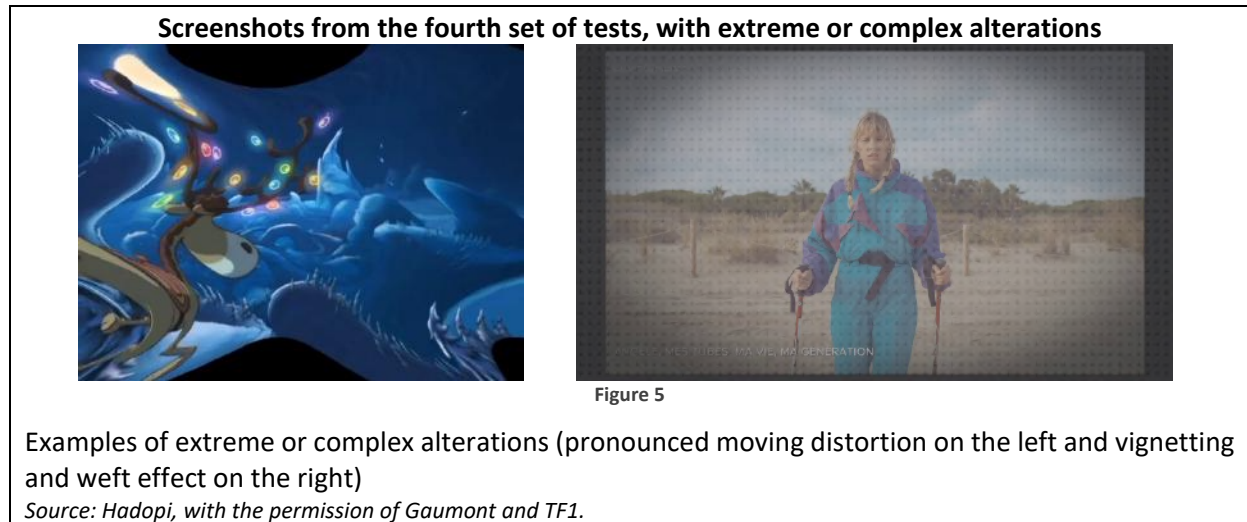
Figure 4

Examples of severe alterations (200% zoom on the image on the left and green-blue hyper-hue on the right)

Source: *Hadopi*, with the permission of TF1.

The top-performing technologies were able to recognise around 90% of the cases submitted in this third set of tests, which is remarkable.

A fourth and final series of tests was made of multiple videos with either extreme alterations or distortions, or combinations of effects known to have effectively thwarted the recognition tools in the past (e.g. darkening of certain areas of the image and addition of a grid of superimposed dots). Some “trick” excerpts, which in theory could not be recognised, were also included in this series.



In the latter series, the technologies success rates ranged anywhere from 50% to 73%. Only cases of extreme modification (in effect making the videos difficult to watch for more than a few seconds) escaped the content recognition tools. In the other cases, the old strategies known to thwart systems were all identified successfully.

To conclude, based on these four test sets reproducing sometimes observed circumvention effects, or effects likely to trip up the content recognition tools, the results were therefore satisfactory overall. Not all the solutions proved equal in the face of the most complex cases; however, this does not seem to be of much concern since the video clips in question, at this level, were so altered that they became unusable.

#### *1.1.1.4. - Identifying fixed images and visual arts works.*

##### ➤ Solutions with different purposes

The solutions applied to fixed images and visual arts works are based on two types of recognition, which should be distinguished according to their purpose. Here, the distinction will be made between those running a fidelity check as opposed to those running a similarity check.

The fidelity check used in particular to identify photographs, artworks or press content involves recognising the same image based on a reference image that may have been partially or totally reproduced and that may have been retouched or modified.

Where applications are concerned, of note is the TinEye reverse search engine, which makes it possible to find on the Internet identical copies of an image submitted by a user, based on an index of nearly



40 billion images inventoried online. The image recognition solutions offered by French company Lamark and by the American company Pixsy also focus on loyalty control.

The purpose of the similarity check is to identify two images that are separate but have the same object or subject and show merely the same thing. These technologies are used, for example, when looking to recognise multidimensional objects and works of art (sculptures, monuments, etc.), but also to recognise decorations and events.

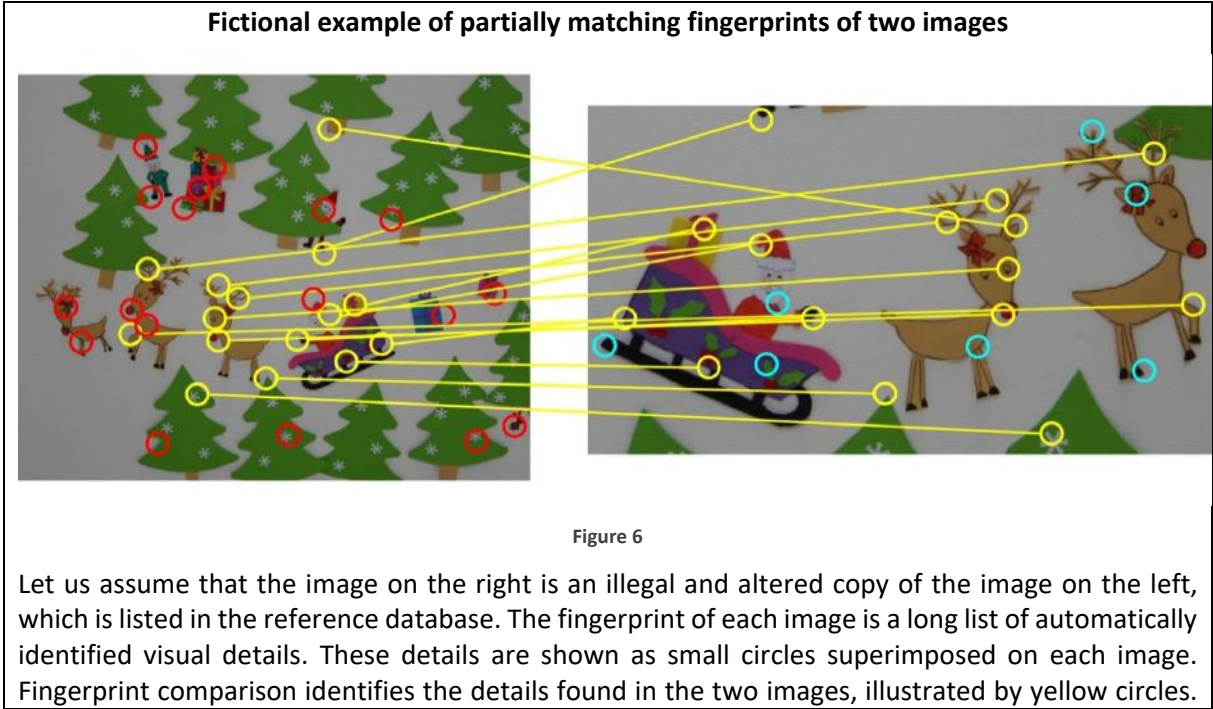
The solution proposed by the Icelandic company Videntifier, which applies not only to fixed images but also video, is more similar to this type of verification and its tool called "VISE" can be used to identify either two separate photographs from the same series of shots, or two photographs that are quite similar but taken by different people in the same place.

Google's reverse image search engine offers a hybrid service capable of both finding faithful copies of a specific image and calling up similar images found on the Internet. However, the technology is not offered to rightholders on Google's own sharing services for the purpose of protecting their works.

➤ How these solutions work

Similar to sound and video technologies, image recognition based on fingerprinting involves excerpting a number of characteristic elements from still images.

However, instead of focusing on pace and motion, still image solutions analyse such aspects as shapes (visible lines, round or pointed objects, etc.) and the way these shapes are arranged between them. The detection of characteristic angles or points in the image, the variance or contrast between certain shades, etc. can also be used as a starting-point.



Those of the left-hand image and found in the right-hand image are connected by lines. Here, matches have been established between many details. The system can thus deem that these two images are indeed similar.

That being said, the system has not matched some of the details. The details shown in red in the left-hand image are not found in the right-hand image, while the details in blue on the right are not found on the left. Note that some details, either blue or red, are nonetheless found in both images. The system was unable to match them. They are false negatives. There is also a false positive in this illustration, meaning an incorrect match. The foot of the tree at the top left is incorrectly matched with the reindeer's ear in the middle right.

*Source: Hadopi and CNRS-IRISA (L. Amsaleg)*

When implemented to verify fidelity, these technologies must go beyond a basic similarity check, which could yield erroneous results. They must also, in order to be effective, more specifically take into account any alterations to the image so that recognition can be made despite the basic alterations or distortions which anyone can end up making when using various software.

When implemented to verify similarity, it is important to focus more on the positioning of the elements with respect to one another on the image, showing a great deal of flexibility. To be effective, the technology will, for example, need to be able to match two shots of the same sculpture or monument, even when the shots were taken from slightly different angles. The solution must also recognise different photos from the same series (for instance, different cyclists riding past a single point) or captured in the same shot (for instance, multiple views of the same cinema set taken from slightly different angles).

Because each solution has its own interests and limitations, it is up to those interested in the outcome to carefully select the one that best suits their needs. Imagine the following situation: two people a few metres away from one another, take a photo of Notre Dame Cathedral burning, at virtually the same time. In the case of a fidelity check, there will be no match between these two shots. In the case of the similarity check, the two photos will be automatically associated because what they show is very similar.

#### *1.1.1.5. - Identifying texts.*

Automatic text recognition appears easier to implement, in particular because the volume of data to be processed when working from raw texts is lower. By way of comparison, the average uncompressed size of an entire novel amounts to around 400,000 characters, where a single uncompressed high-definition image contains more than 2,000,000 pixels.

Text recognition can be applied to both literary writing and uncompiled computer code, i.e. represented in a readable format, including STL-format stereo lithography files describing 3D objects.

The digital fingerprint of a document can therefore be its conversion into raw text, once the layout, style effects, tags or other items have been removed. The processes capable of converting images into



raw text (i.e. optical character recognition, or "OCR"), have been in existence since the 1950s and can now make it relatively easy to convert large volumes of digitised documents into raw text.

Internet search engines, in particular those enabling text searches in referenced publications, can to a certain extent be referred to as automatic text recognition tools: based on an excerpt or a few isolated words, the tool is able to very quickly find texts containing the passage searched for or containing – in a more or less similar manner – the different terms requested.

Similarly, powerful search engines are able to match multiple texts even when these have been subject to alterations. For example, a search on Google.fr for “ootli de reconai5ance de c0ntenus” [equivalent of “searth recogni5ion t0ols”] will automatically be interpreted as a French-language search concerning such content recognition tools and the top eight search results in fact relate to the CSPLA / Hadopi / CNC mission with which this report deals (based on a test carried out in October 2019).

Digimarc, a U.S.-based identification solutions provider for the fight against counterfeiting and piracy, acquired Attributor Corporation in 2012, which offers a content recognition solution adapted for text searches. The publisher Elsevier also offers a solution called Fingerprint Engine, but the aim of which is more to match up different texts by themes they have in common.

It can be noted, lastly, that some text search engines are focused specifically on detecting plagiarism. The purpose here is no longer to compare texts word for word or to take into account clever letter substitutions, but rather to match texts using synonym dictionaries, detect changes in the order of phrases, shifts from the active to the passive voice, etc. These engines are used in particular by editors of scientific publications wishing to identify in a paper being considered for publication any material that might come directly from previous contributions.

#### *1.1.1.6. - Identifying video games.*

Applying automatic content recognition to video games, as to other software and computer applications, is always quite complex.

One of the difficulties comes from the fact that most video games and software distributed online come in the form of compiled, compressed and fragmented files, which are very difficult to analyse.

However, computer program recognition technologies can also be built on the same principles as antivirus software, which analyses files and documents to detect the possible presence of malicious or dangerous computer code in one form or another.

Analyses performed by antivirus software can be likened to recognition of (in this case harmful) content embedded in computer files, from a reference base made up of known computer viruses and malware (in which case, the term used is "signatures" rather than fingerprints, although the two concepts are quite comparable). It therefore does not seem totally incongruous to think that the same technique could work for the recognition of protected computer programmes.

Some digital platforms offering the ability to store all kinds of files online, such as the Google Drive service, or app stores such as Google Play and Apple's App Store, are already using antivirus scanning

tools today to make sure that no malware is integrated to games, programs and applications that are made available.

The same principle could by the way apply to the recognition of virtual reality works, which are most of the time interactive programs<sup>11</sup>, distributed online through dedicated platforms that are still emerging but on the rise. These new types of contents can thus be considered as video games made for specific VR devices and, likewise, they can be analysed and protected in the same way as video games.

## 1.1.2. - Other supplementary methods with more limited effectiveness.

### 1.1.2.1. - *Hashing: limited to recognition of strictly identical content.*

*Hashing* is a technology first developed in the 1950s, and now widely available in open access. It consists in representing a data item or computer file with a single alphanumeric character string. A *hashcode* is thus a kind of unique signature. The idea is to transform data or a file (for example a password or an image, video or audio file – whatever its size) into a series of 32 (for the MD5 standard) to 128 (for the SHA-512 standard) characters.

Two strictly identical files will thus always have the same *hashcode*. The function is not reversible: the original content cannot be “recreated” from the *hashcode* alone.

Moreover, it is almost impossible to find two separate files for which the hashing function would generate the same *hashcode* (this is referred to as a collision). The hashing-based file recognition technique is therefore very reliable.

When a file is reported as in violation of the law, its *hashcode* can be calculated and added to a reference list. If another file (already on the platform or subsequently put online) has the same *hashcode*, it can be assumed to have exactly the same illegal content and should thus be blocked. This summary blocking technique, known as *take-down stay-down*, is used by Dailymotion as well as some file hosting platforms.

However, this technology offers limited value when it comes to protecting intellectual property rights, as a file that is not exactly identical to the reference file will not be recognised.

This technology is thus not sufficiently flexible. The slightest change in a file (single character in a text removed or replaced, single pixel on an image changed, very short passage in a sound file removed or added, format changed, etc.) will result in an entirely distinct *hashcode* and the illegal content will not be detected.

---

<sup>11</sup> Besides interactive VR works, there are however linear contents made for virtual reality (for instance, immersive videos showing 360° images, possibly in 3D). Videos of this kind can already be distributed on platforms such as YouTube. With regard to this specific type of linear content, the making of video fingerprints to enable automatic content recognition seems feasible because, even if the VR video format is quite peculiar, it is generally a simple panoramic image that has been flattened, sometimes split in two for the 3D effect.

### 1.1.2.2. - *The use of metadata on platform search engines enables a basic but fragile form of content identification.*

Metadata is data used to define or describe another data item.

There exist dozens of examples of metadata related to digital media: the date of creation of content, author of a photograph and GPS coordinates of the location where the image is taken, names of authors, performers and producers of a sound recording, title of a work, version number, keywords related to the content, etc.

Metadata can be directly integrated into the files containing the works, depending on their format (this is possible, in particular, with images or mp3 audio files). They can also be stored in a separate database, provided there is an identifier to connect each piece of content with its metadata. A simple query in the database, provided that this information has been entered in advance, can identify, for example, all content created before a given date, or find all works created by the same author, or all paintings the title of which contains a particular word. Today, the latest algorithms can find not only exact matches, but also close matches (e. g. when accents are missing or words are slightly misspelled).

However, to be truly operable, the structure and format of the metadata must follow commonly accepted standards. This is not always the case today, especially with digital photography where different standards coexist.

Moreover, these are very fragile, low-security systems insofar as metadata can easily be altered, modified or deleted.

The technology is also not entirely reliable. In particular, care should be taken with the risk of homonyms. The name Pierre Richard may for instance be that of the much-loved comedian and screenwriter behind the film “I don't know much, but I'll say everything” or a MP for the Seine Region from 1893 to 1903 who is the author of the book “*Le process de la Ligue des Patriotes*” (“The Trial of the League of Patriots”)he. Similarly, the title “The Lord of the Rings” can be that of the fantasy novels published mid-twentieth century, the series of films released in the 2000s or a yet to be released television series. The identification of content solely on the basis of metadata therefore requires caution and generally requires manual verification or multiple cross-referencing.

Lastly, in addition to possible reasons rooted in the protection of privacy, it should be noted that many digital platforms tend to remove, on practical grounds, all or part of the metadata from the image files they host. While the weight of metadata is quite insignificant for a feature-length video, it is not negligible with a miniature photograph (500 uncompressed metadata characters can amount to as much as 10 or 20% of the total weight of an image in the form of a compressed thumbnail). However, the removal of metadata for technical reasons is no longer truly warranted in the age of broadband Internet connections.

### 1.1.2.3. - Watermarking or digital marking: a solution with multiple uses but little-used on platforms.

#### ➤ Description of technical functioning

Digital watermarking is the process by which a specific signal is integrated into content, and which can later be retrieved. It is a kind of signature integrated into the work, and makes it possible to identify, thanks to a tool capable of detecting it, the originals and copies made of them.

Two instruments are essential to implement this technique:

- a marker, the role of which is to mark the content,
- a detector that analyses the content to see whether it has been watermarked.

Watermarking implies a modification to content so that it can be subsequently verified. A watermark can be visible (or audible when the content is a sound file), such as when a logo or inscription is added to an image or video. It can also – and this is increasingly the case – be invisible to the naked eye (or inaudible in the case of sound) while remaining perceptible to the detection module.

For video content, watermarking will involve modifying the flow of images by playing on components or details generally imperceptible to the human eye. Watermarks can be inserted at regular intervals or can be looped throughout the content. The same goes for audio, where waves or distortions which the human ear does not (or can hardly) sense are added to the audio signal.

As regards still images, watermarking means adding a mark or a kind of invisible filter, which can for example play on the luminance of each area of the image.

Where documents are concerned, it is also common practice to add a watermark. It is even possible to watermark raw text by slightly modifying it (for example by adding double-spaces at specific locations or by replacing the letter "O" with the number "0" or the capital letter "I" with lowercase letter L "l" at a given location).

In the case of software, applications or video games, one technique likened to digital watermarking consists of integrating into the programme *package* (i.e. in all the data that make up the computer programme) an image or a distinctive identifier that can then be found by analysing the said *package* or just running the programme.

#### ➤ Purposes of the said technologies and existing offers

Digital watermarking can be used to enable video, sound or image recognition. The French companies Content Armor and Nexguard (acquired in 2016 by the Swiss group Kudelski), or the US company Verimatrix are just some of the suppliers of these technologies.

Historically, this technology was used in the film industry to trace, after the fact, the party responsible for a leak, for example in the event of unauthorised distribution of a working copy or illegal capture of a film shown in the cinema. If the pirated copy of the film is analysed, the watermark and therefore the original recipient of the leaked copy can be found. This leads back to the source of the incident. In

this case, watermarking has been used as a deterrent, with an individualised marking (referred to as a "session-ID" or "user-ID" type mark).

There exist other forms of application, such as generic watermarking of content broadcast on television. In that case, all of the contents' recipients receive the same marked signal. The marking may include information about the broadcaster and possibly timestamp data (referred to as "network-ID") in order to detect whether content has been broadcast by a specific television channel and, if so, on what date.

Digital watermarking is thus a technology that is already significantly developed and widespread for certain uses, but still relatively little used for the detection and recognition of protected content, particularly on digital platforms. For several years, however, various major players in the audiovisual and advertising sector, in particular through organisations such as the Society of Motion Picture and Television Engineers (SMPTE), the Coalition for Innovative Media Measurement (CIMM) and the Entertainment Identifier Registry Association (EIDR) have been working on standardisation projects.

It should be noted that the International Standard Audiovisual Number (ISAN), a universal identification number for works like the EIDR, adopted mainly by European countries and made mandatory in France for works assisted by the CNC, can serve as an identification reference number for watermarking works and versions thereof.

This type of watermark, in which the work's identifier is incorporated into the content, can also be called "content-ID" insofar as it does not in this specific case identify the recipient or its broadcaster.

This system is used in particular for television advertisements in order to automatically count how many times a particular advertisement has been broadcasted on air over a given period. Kantar Media, which acquired the *watermarking* audio solution Civolution, also uses this technology to measure television audiences and monitor television programme broadcasts in France: audience measurement boxes from Médiametrie analyse the audio watermarking found in the programmes viewed by the panel of viewers to determine which channels are watched.

With certain techniques, multiple markings of the same kind can be incorporated within a single content unit, without cancelling each other out, or deleting previous versions as they appear. It is therefore possible that one or more "content-ID", "network-ID" and "user-ID" type watermarks be placed on a given piece of content. It is also possible that multiple types of different watermarks be placed on the same content without causing any problem (as each solution normally has its own specific features).

The possible accumulation of markings is useful during post-production of audiovisual works: each subcontractor receiving protected elements applies (or is tagged with) a digital watermark, thus making the content that passes from hand to hand fully traceable.

Lastly, it may prove worthwhile to watermark images or soundtracks for the live broadcast of sports competitions. The insertion of a distinctive watermark in content broadcast live, at the source, can make it easier to automatically detect a pirate stream broadcast live on a sharing platform. If the

stream in question contains the distinctive marking, then it is probably a re-broadcast of the protected programme.

### ➤ Efficiency challenges

To be considered effective, a digital watermarking solution must be able to easily generate and then detect the marking. The solutions must have light technical resource requirements, so as to be suitable for large-scale deployment. Any copy bearing the mark will therefore be immediately detected. On a large scale, however, the nature of the marking must be diverse enough to keep simple statistical tests from revealing its presence. If a million images are all tattooed in the same way, then the mark will be relatively easy to find. Frequently changing marking settings in order to ensure great diversity makes watermarking expensive and the detection process more complex, as many combinations need to be tested.

These technologies must also be sufficiently robust and resistant to conversions, slicing, compression, re-encoding, signal deterioration and other geometric distortions. When they are not, people with sufficient knowledge and skill can successfully blur or erase digital markings, including by merging several distinct marked versions together (this is known as a collusion attack). There also exist specialised watermark algorithms that are resistant to such collusion attacks. They are complex and expensive.

Furthermore, a copy not bearing any mark, for example if it was created prior to the watermarking operation, will not be recognisable by the system. Watermarking cannot therefore be applied retroactively, and serves only to protect new streams of marked content (not the stock of unmarked copies already in circulation).

Besides, the large-scale use of digital watermarks is worrying some actors, who fear that the robustness of the technologies could diminish if too many actors have access to the marking detection module. Ill-intended individuals could attempt, through reverse-engineering, to reveal the system's detailed workings and thus weaken it.

In conclusion, despite a certain fragility in the current tools, digital watermarking offers advantages and can therefore be complementary to digital content recognition systems based on fingerprinting in meeting needs that are unique or poorly taken into account by fingerprints.

Some approaches (like that of the French company Lamark) indeed combine similarity-based searches with watermark detection. Lamark thus analyses all similar images identified by the search engine and attempts to detect any watermarks they may bear. If the latter is found, then it becomes certain that the image is indeed protected and is not a false positive. This approach is very beneficial and provides conclusive evidence of ownership.

1.2. – The practicality and the sharpness of fingerprint content recognition technologies can be assessed by analysing their implementation.

1.2.1. - While recognition tools are already extensively used, deployment still varies depending on the players and sectors.

The decision made by the most significant platforms in favour of large-scale fingerprinting systems for audio and video contrasts with that of other players and sectors.

*1.2.1.1. - A model based on digital fingerprinting has established itself on the platforms geared towards audio and video*

The platforms dedicated to audio and video have opted for a model that uses digital fingerprint recognition to initially block unauthorized content and then move gradually to a monetisation approach.

In 2007, two years after their launch, YouTube and Dailymotion became the first platforms to use digital content recognition tools based on fingerprinting.

YouTube started out working with Audible Magic, before deciding to develop its own audio and video fingerprinting system, now known as Content ID. In the summer of 2018, YouTube launched the “Copyright Match Tool” solution, a scaled-down version of Content ID for users signed up for its partner programme to track videos that take back all or part of their content or to request that unauthorised copies of their content be removed. In addition, YouTube now uses other tools to analyse content uploaded by Internet users (analysis of lyrics and images using artificial intelligence) but for purposes other than the recognition of protected works.

The platform DailyMotion chose to use technologies developed by third parties, namely Audible Magic for music and the INA for video. The platform continues to use these third-party services but has, in recent years, been developing in addition an internal tool called “Content Protection System” (CPS), derived from the system developed by INA, INA-Signature. DailyMotion’s CPS uses a dedicated fingerprint reference base to enable content to be monetised with certain partners. Dailymotion also uses the “hashcode” filtering technique to prevent files that have already been flagged and blocked in the past from being put back online.

The Twitch, TikTok and Soundcloud platforms appear to be working primarily with Audible Magic for audio content recognition but without using a video solution.

Blocking measures based on metadata may occasionally be implemented on certain platforms, particularly during sports competitions, in order to limit the visibility of videos likely to broadcast matches live.

Video sharing platforms specialised in pornographic content, such as Pornhub, Youporn, xHamster and XVideos are also interested in content recognition technologies, again using mainly digital fingerprint-

based tools for blocking purposes. In particular, rightholders can ask XVideos and PornHub to generate fingerprints of their productions free of charge to prevent them from being posted on these platforms or on competing platforms.

### *1.2.1.2. - Mainstream platforms are still uneven in their adoption of digital fingerprint recognition solutions*

Facebook is the only global mainstream platform known for having decided to develop its own content recognition tool, called Rights Manager, after initially working with Audible Magic. Launched in 2016, the Rights Manager tool makes it possible to generate audio and video fingerprints of protected works and then to have content blocked, monitored or monetised.

Facebook has also developed image and video comparison algorithms (called “PDQ”<sup>12</sup> and “TMK+PDQF”<sup>13</sup>) through the work carried out by the team of the Facebook Artificial Intelligence Research (FAIR) centre based in Paris, in cooperation with the University of Modena and Reggio of Emilia. In August 2019, Facebook decided to make both these technologies available to the public in open source in order to improve the fight against illegal content, particularly child pornography. However, these solutions are not used by the platform for the recognition of copyrighted works.

Besides, Facebook uses internally other content analysis tools, based on artificial intelligence, but once again for other purposes than the protection of author rights and related rights.

The Russian social network Vkontakte (or VK) has also implemented a video *fingerprinting* tool in recent years. It chose Audible Magic's solution for video while leaving open the option of developing its own solution.

On social network Snapchat, it would appear that no content recognition tools are implemented.

While LinkedIn and Twitter have not communicated at this stage about the implementation of content recognition tools, these platforms impose limits on the length of the content which users can share. Twitter also has tools for detecting fake accounts and fake news and is said to be working on tools to recognise offensive or terrorist content.

### *1.2.1.3. - Platforms dedicated to image do not implement fingerprint recognition systems on their own*

While solutions do exist, they seem to be little implemented by the main platforms dedicated to images on the Internet (Instagram, Pinterest, Flickr).

---

<sup>12</sup> PDQ is a “Perpetual” spectral hashing algorithm, which uses a Discrete Cosine Transform producing a Quality metric.

<sup>13</sup> TMK stands for *Temporal Matching Kernel*.



In practice, rightholders and their representatives therefore monitor digital platforms themselves by searching for specific works, most often using metadata-based queries. They can then request that any unauthorised content be blocked.

Instagram, a subsidiary of Facebook, has made efforts in the field of content detection, but with the aim of detecting offensive or violent images, images involving nudity, as well as inappropriate texts and comments posted on the platform by users or, for instance, unwanted advertising (spam).

To date, the Pinterest platform does not appear to have implemented a detection system on its service for the purposes of protecting copyright or related rights.

Since April 2019, Flickr has offered its “business” members a service detecting stolen photos, working in partnership with the company Pixsy: users subscribing to Flickr’s paid offer can thus protect up to 1,000 images. Pixsy then undertakes to search for possible unauthorised copies of these images all over the Internet (content recognition is therefore not limited to Flickr).

#### *1.2.1.4. - On platforms dedicated to text, almost no recognition tools are in use.*

Although the appropriate technologies do exist, automatic recognition of protected content is not widespread on digital platforms dedicated to textual works. And as with still images, there is no very extensive reference base in this area.

The platform Calaméo dedicated to sharing publications online, which has more than two million monthly users in France alone, and the international platform Scribd, which presents itself as a digital library, do not offer a tool for analysing content posted online by Internet users. However, Scribd invites rightholders to use third-party solutions such as Digimarc, DMCA Force, MarkMonitor or Red Points or the Google Alerts service. Google Alerts, for example, is able to detect text or a string of characters on platforms such as Scribd and offers one-time or recurring alert mechanisms if matches are found.

With regard to the scientific publications sector, RELX/Elsevier has developed a content recognition solution which it uses on its own platform ScienceDirect. This solution has also been tested on the independent platform ResearchGate but, according to the latter<sup>14</sup>, the experiments have not yet yielded conclusive results.

---

<sup>14</sup> Contribution of Researchgate to the consultation of the German Federal Ministry of Justice and Consumer Protection in September 2019, in relation to EU Directives 2019/790 and 2019/789: [https://www.bmjj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2019/Downloads/091619\\_Stellungnahme\\_ResearchGate\\_EU-Richheberrecht.pdf;jsessionid=337BDA34E02D03657A54E8EDA70F5970.2\\_cid289?\\_blob=publicationFile&v=2](https://www.bmjj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2019/Downloads/091619_Stellungnahme_ResearchGate_EU-Richheberrecht.pdf;jsessionid=337BDA34E02D03657A54E8EDA70F5970.2_cid289?_blob=publicationFile&v=2)

1.2.2. - There exist several ways of organising tools that go beyond the models developed internally by some platforms for their own use.

The different platforms that have developed internally their own content recognition solutions, as well as third-party service providers, seem to have all adopted their own format and standards, without consulting with the others. Beyond the implications relating to these different modes of organisation and notwithstanding the development of new detection tools, this heterogeneity risks making rightholders' tasks more difficult, without a certain standardisation.

*1.2.2.1. - The use of internally developed fingerprint systems by platforms is the model chosen by dominant players and has proven its feasibility for large-scale implementation*

➤ How the solutions originated

Owing to the high profile of their respective developers, namely YouTube and Facebook, the Content ID (and its lighter version Copyright Match) and Rights Manager tools enjoy particular visibility in the field of content recognition. They stand out mainly for being integrated directly and in optimal fashion into digital platforms and being developed by the platforms themselves, internally, and not by third parties.

Dailymotion's "content protection system" also referred to as "CPS", although based on INA's digital fingerprint technology, can also fall into this category of internalised tools.

This model has the advantage of drastically limiting the number of intermediaries involved in the operating chain. A rightholder can therefore, just by using the YouTube or Facebook interface, send to the system any content for which they wish to generate fingerprints, define the related management rules, review the videos that match their fingerprints, monitor the monetised content, manage conflicts and contestations, etc. The use of these tools is generally free of charge for rightholders.

This organisation mode carries the following implications:

- the platform alone manages the content recognition technology, the way in which it is used and how it evolves;
- Rightholders must learn to understand in detail how the tools operate, both in terms of conflict arbitration between fingerprints, the workings of the monetisation system and methods for managing user contestations;
- The platform may require rightholders to provide the content from which the fingerprint can be generated, or at least the fingerprint itself as well as specific information (title, author, etc.) so that the content can be identified, failing which the right to use the recognition tools may be refused.

## ➤ Fingerprint management procedures

The platforms generate the fingerprints for the content to be protected. This operation is generally free of charge for rightholders and is carried out using a dedicated interface called “CMS” (for content management system).

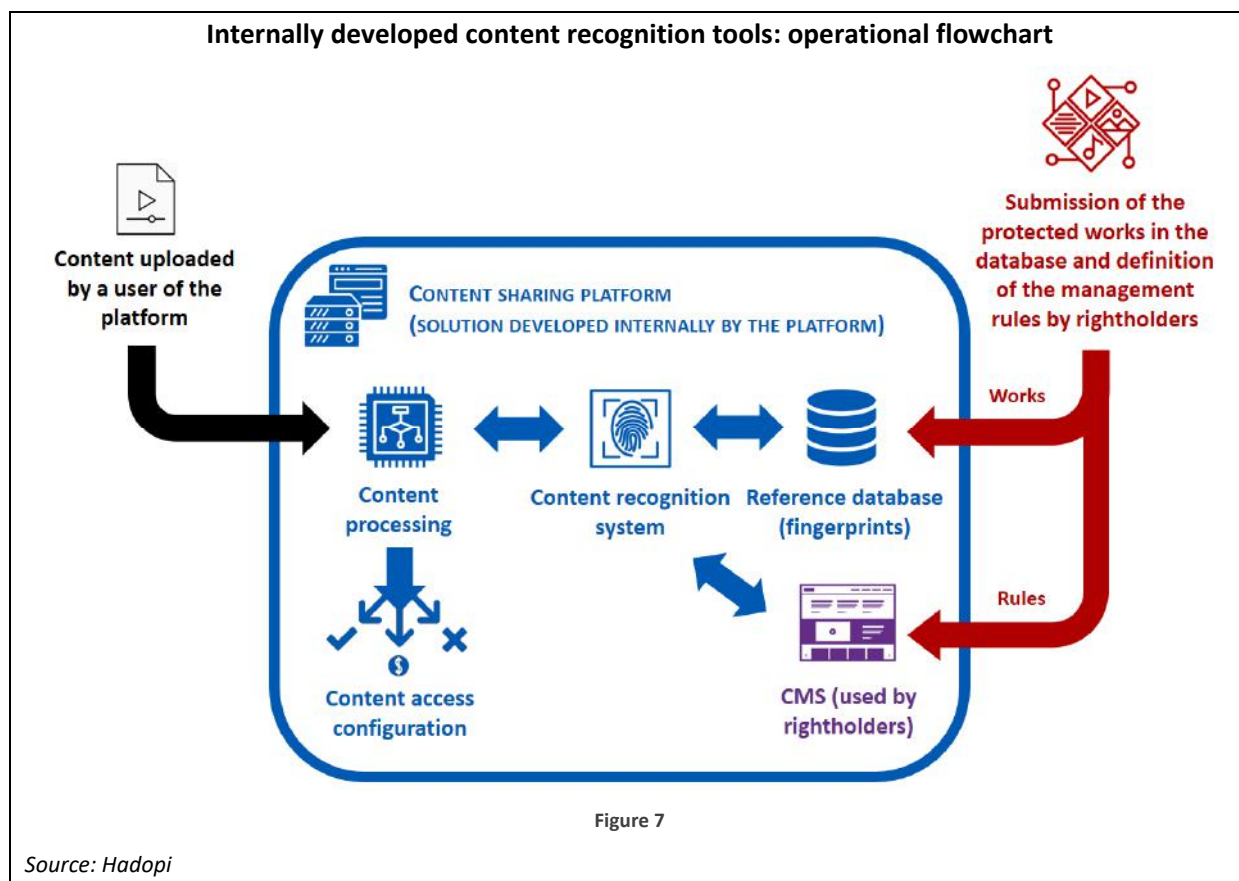
This operation also entails entering a certain number of metadata, in particular the title of the work. For certain rightholders with substantial music or video catalogues, the mass transmission of source files and metadata to the CMS can be made automatic, provided that certain formatting procedures imposed by the platforms are followed.

Some services, including YouTube, may also offer a software tool, used in particular by film producers, that can generate fingerprints for Content ID externally, without requiring that a unprotected copy of each content item be addressed to the platform. It would appear that Facebook is also offering this feature to certain rightholders, even though its representatives clearly stated to the Mission their preference for content to be sent to the platform by rightholders themselves.

The Content ID system does not offer full back-compatibility for externally generated fingerprints, whereas the Content ID fingerprint model is usually updated at least annually.

It follows that when the fingerprint system is updated or when a technology is changed by a platform such as YouTube, the rightholder who has chosen to generate its fingerprints externally must recalculate - for the entire protected catalogue - a complete set of new-generation fingerprints, if it wishes to continue to benefit from optimal protection. Conversely, as soon as the platform has the original files, it can directly generate the new fingerprints internally.

YouTube believes that only the latest and penultimate generation of Content ID fingerprints should remain operational. Less effective fingerprints, made with older versions of the fingerprint generator, are no longer taken into account and are deactivated as new generations of fingerprints come into use.



1.2.2.2. - *Third-party tools, already used by certain rightholders, may also satisfy content recognition needs on sharing platforms.*

➤ How the solutions originated

A second organisational model when it comes to content recognition is the use of one or more third-party technologies by the platform. Companies specialised in content recognition most often develop these technologies. They can be integrated on the platforms by paying a license fee: this is the case, for example, for the solutions proposed by Audible Magic and Ina.

The benefit for a platform in acquiring third-party solutions is the ability to delegate content recognition tasks to external entities.

In practice, for each content uploaded, the platform generates a fingerprint in a format defined in the specifications of its service provider, then sends this fingerprint to the third-party content recognition system managed by the service provider. After analysis, the service provider's system informs the platform of any matches and issues the appropriate instructions (blocking, monetisation, etc.). It is up to the third-party service provider to make sure that he has a sufficiently complete reference base to remain competitive. The addition of fingerprints to these third-party reference databases is generally free of charge for rightholders.

This organisation mode carries the following implications:

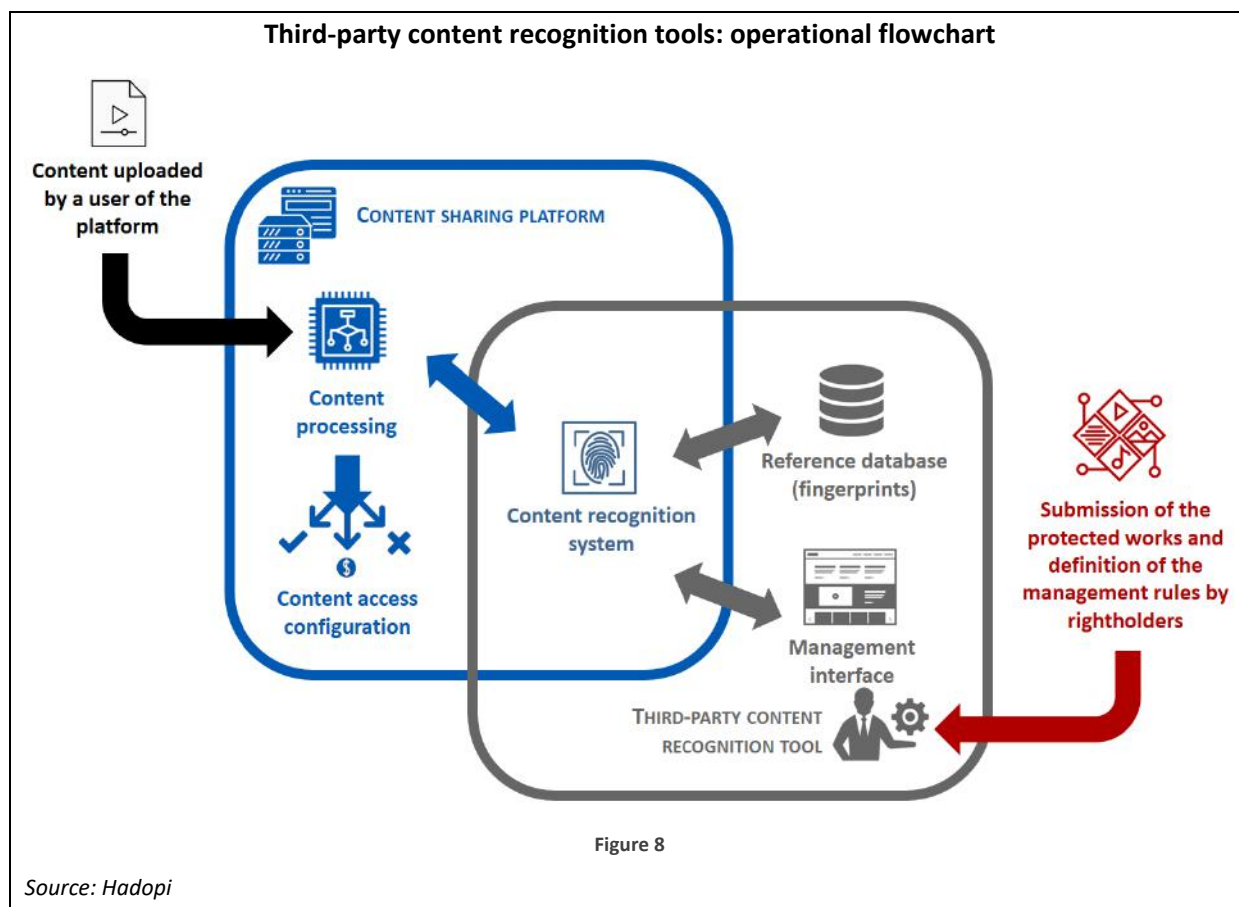
- for platforms, it offers greater flexibility or makes it possible to avoid or limit solution developments internally;
- a platform may use multiple complementary third-party technologies;
- this organisational model makes rightholders less dependent on the platform's choices, even if the platform remains the decision-maker for the choice of service provider;
- the involvement of intermediaries offering third-party technologies can complicate the resolution of malfunctions on a platform, because the investigations required to understand the origin of a problem require consultation between the platforms, the technical solution provider(s) and the rightholders.

Other technologies may also be used independently and as a supplement, by the rightholders, at their own expense, including where the platform has its own internal solution, in order to scan and analyse externally contents available on the sharing platform, but only those made public (offers proposed for example by the companies Vobile, PEX and Lamark, although these tools could also be integrated on the platforms).

#### ➤ Fingerprint management procedures

In most cases, the content protection providers that have developed their own technologies are responsible for making fingerprints for their reference base from the works made available to them by their customers. If necessary, the content is transferred from the rights holder to the service provider via a secure connection and the service provider may undertake, for security reasons, not to retain the files permanently, once the fingerprints have been generated.

It is also sometimes possible for the service provider to provide rightholders with an application capable of generating fingerprints locally (at the rightful owner's premises): this is for example the case of the Ina, which authorises its clients to generate a fingerprint of the sensitive content externally, then send this fingerprint to the INA-Signature database. The Ina, whose technology is regularly evolving, then ensures that its system is backward compatible with the old generation fingerprints generated externally.



### 1.2.2.3. - The answer to the problem posed by the multiplicity of systems.

In view of the multiplicity of platforms on which content must be protected and the increasing number of solutions available to provide effective protection, rightholders are subject to multiple and restrictive due diligence procedures. However, complementary or alternative organisational models may be able to overcome these difficulties.

#### ➤ Centralised service provision (one-stop shop, “universal fingerprint”)

Various so-called “delegated” or “one-stop shop” services have appeared on the market in recent years, offering rightholders the opportunity to have their content protection managed centrally. The French company Blue Efficiency, for example, offers this type of service under the name “universal fingerprint”, not to denote a fingerprint format compatible with different *fingerprinting* systems, but to designate a single service to manage multiple content recognition tools through a single portal.

Following the signing of a partnership agreement between the Association for the Fight against Audiovisual Piracy (ALPA) and Google on 19 September 2017, under the aegis of the CNC, a one-stop-shop system was set up to protect the works of ALPA members on video sharing platforms such as YouTube.

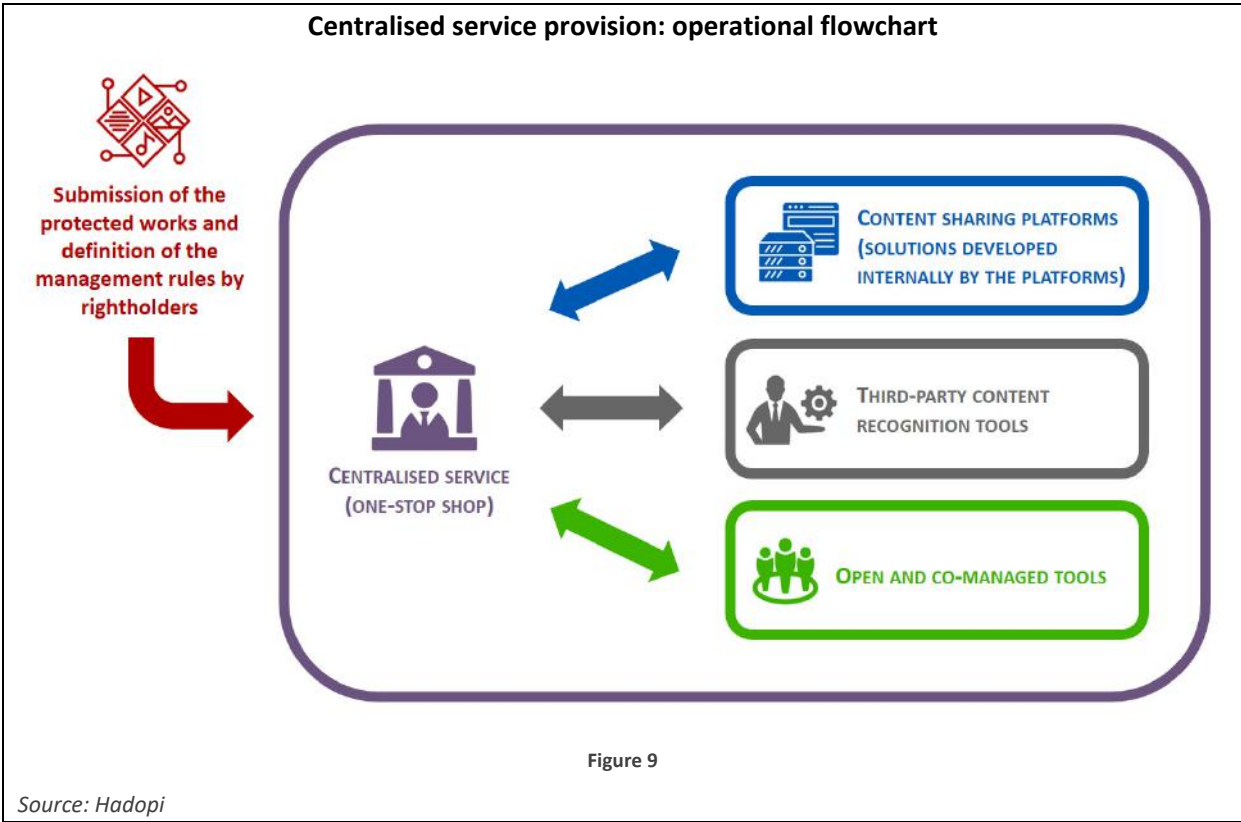
In practical terms, rightholders delegate the management of their fingerprints and content on the main sharing platforms to content protection specialists.

The main purpose of the centralised service providers is to address rightholders of modest size or who do not wish – due to a lack of expertise or resources – to manage the protection or monetisation of their content on online sharing platforms themselves.

Through a single, specialised entity, rightholders are therefore able to protect or monetise their content both on tools developed internally by major platforms such as YouTube and Facebook and through third-party tools integrated into various platforms, such as those made by Audible Magic or open and co-managed tools (see next point).

Without establishing any interoperability between the systems in place, this type of service provision does allow rightholders to have their content protected on multiple platforms - by entrusting a single entity with their works and management instructions.

Such a service comes at a cost for rightholders, unlike most of the organisational models presented above. However, the one-stop shop offered in France by ALPA to its members bypasses this difficulty since this service is shared and financed by the profession, with the help of the CNC and, at times, sharing platforms: all direct or indirect members of the association can benefit from this service at no extra cost.



➤ Is developing open and co-managed tools a feasible solution?

In an effort to pool efforts, simplify tools and improve transparency, some digital actors such as the Qwant search engine are advocating for the implementation of a community management system for content recognition. However, this method of organisation does not yet exist on a large scale and remains to this day at the project stage.

The main idea here is that of developing a common interface, in open source, using proven content recognition technologies from the public domain. The proposed system would be able to process fingerprints of musical, audiovisual, literary, photographic works, etc. Rightholders could register their works in this centralised system free of charge, then place their fingerprints in the central reference base.

They would also be able to enter their preferences in the system as concerns the rules for blocking or monetising their works (via sharing advertising revenue or by claiming a fixed amount for each use of their content items). The system, either self-managed or administered by a neutral entity, would be responsible for resolving any conflicts between fingerprints and between the rules defined by the users of the system.

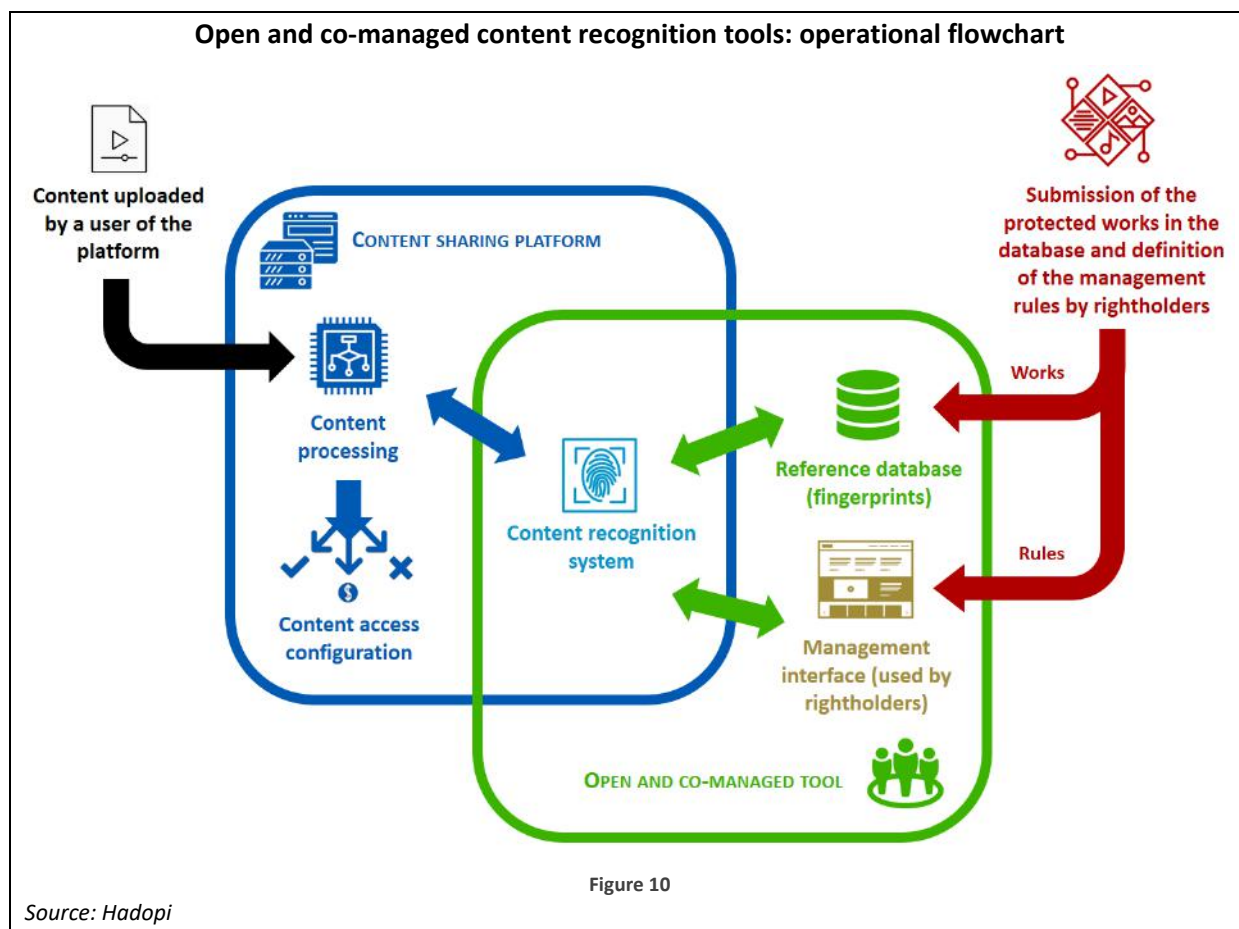
Platforms, for their part, would be able to analyse all the content posted online by their users thanks to this shared tool. The cost of the licence for benefiting from this service would be limited and would only be used to finance system maintenance and the technical resources necessary for its operation. This solution could be used as a complement to the tools already used by the platforms. It could also eventually replace them.

The major advantage of this system lies in its being open to all and in the balanced model it offers between platforms and rightholders. It is, moreover, the method of organisation that is closest to the interoperability solution for which some are calling, but which technical constraints make difficult to implement, each commercial fingerprint recognition solution having its own characteristics.

On the other hand, difficulties could arise with the governance of a tool involving so many stakeholders and given the legitimate doubts that can be raised about the ability of such a multiparty system to self-regulate. The impact of such a model could also have significant consequences for all the actors already operating in the content recognition market, in particular by limiting the incentive to innovate further.

Lastly, the relatively open and transparent operation of the system should serve as a call for great vigilance, particularly if the technologies used for content recognition prove vulnerable. Here, it is the entire tool that could be hurt by a malicious attack or failure.



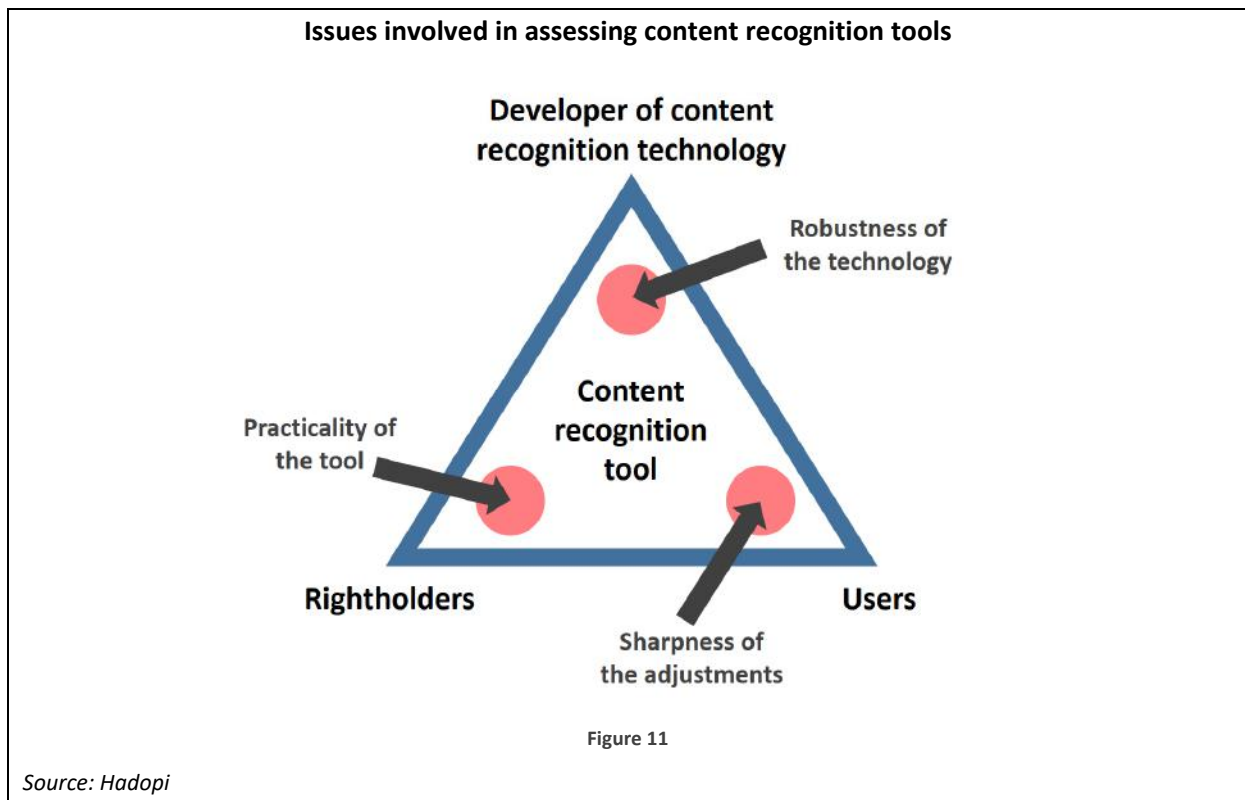


### 1.2.3. - A closer look at the detailed functioning of the tools with regard to their practicality and sharpness.

A thorough analysis of existing tools based on digital fingerprinting enables the identification of key parameters of their effectiveness. Analysis focusing on the robustness of recognition technologies alone is not enough to gain a complete understanding of their overall effectiveness, as other aspects must be taken into account, such as practicality and sharpness.

Practicality refers to the ability of a technology and its interface to be used simply and efficiently by rightholders; this involves examining the functionalities offered – or not offered – by the various tools and the ease with which they can be used. These functionalities are intended to improve the various options for rightholders in setting the CMS criteria for each work in order to reduce the number of identification failures, better manage incidents, and identify and resolve cases of conflict.

Sharpness refers to the ability, by adjusting the parameters offered by the solution, to distinguish between presumed violations of rights and legitimate uses of pre-existing works (in particular in the context of exceptions to copyright), so as to avoid removing or unduly blocking content.



*1.2.3.1. - Some functionalities make it possible to limit conflicts and address cases of fingerprint redundancies for the same protected content, right from the fingerprint generation stage.*

Current tools, which are focused on the recognition of content by digital fingerprinting, mostly rely on a reference base in which the fingerprints of protected works are stored. The more complete this database, the most relevant it will be. This database must also be able to be continuously and easily completed with new fingerprints. The richness and freshness of the catalogue are therefore an essential criteria for assessing content recognition solutions.

The CMS offered by YouTube and Facebook include so-called “deconfliction” features to deal upstream with redundancies between the new integrated fingerprints and those that already exist.

Providers such as Ina and Audible Magic also take on the task of resolving any redundancies between fingerprints submitted by their customers, in order to maintain consistent reference bases.

In some cases, redundancies can be explained by the fact that a work is composite or contains a passage found in other already referenced contents (for example, the credits of a TV series are often the same from one episode to the next). It is therefore important that recognition tools be able to exclude a segment from a fingerprint in order to limit conflicts.

In other cases, the conflict may arise because one rightholder only has rights over a content in some countries, while another covers other territories.

The most effective fingerprint reference bases are those that reflect these specificities in order to avoid potentially contradictory instructions between the respective rightholders or to at least warn and put in contact as soon as the fingerprints are generated the different parties involved in a conflict, so that they come to an agreement on who is the true owner of the rights and who must take control of the original fingerprint. It is important that the conflict resolution interface be simple to use to facilitate and streamline exchanges.

When a conflict persists despite the dialogue procedure, the manager of the content recognition tool arbitrates, and one of the fingerprints is generally deactivated (often the most recent, although some systems prefer to deactivate the oldest fingerprint).

### *1.2.3.2. – Analysis of the ability for rightholders to define and fine-tune management rules.*

Once the works are submitted in the form of a fingerprint in the reference databases, it is up to the rightholders, within the limits of the possibilities offered by the recognition tools, to define the rules to be applied when content uploaded on the platform matches a reference fingerprint, in full or in part.

- The main content recognition systems today tolerate the creation of multiple rules that can be overlaid or can complement each other for a single content item

Rightholders may generally choose between three or four basic actions in order to manage how their contents have to be processed by sharing platforms.

For instance, they may block protected content so that it is not visible on the platform.

They may also authorise its distribution in exchange for a share of the advertising revenue which the content might generate on the platform (this is referred to as content monetisation).

Rightholders may also authorise the sharing of content without compensation and just track (or monitor) the content.

Lastly, they may request a manual review of the detected content in order to decide on a case-by-case basis which rule to apply.

These actions are referred to using the generic term “claims”. A claim is the act by which rightholders seek power of control over the way in which their content can be disseminated on a platform. While some content recognition mechanisms currently offer no more than blocking of protected content, others are more advanced and offer more options.

In the case of recognition tools developed internally by digital platforms, the claims rules (or methods for processing matches) can be added and modified by the rightholders at the CMS level. Platforms sometimes reserve the right to grant certain functionalities only to certain rightholders, at their sole

discretion. These restrictions may relate, for example, to the minimum duration of an excerpt beyond which an automatic rule can apply, the ability to define rules applied solely to sound or image, or the obligation to manually review all correspondence during an initial period referred to as the “trial” period.

In the case of third-party recognition tools offered by service providers, rightholders generally provide the service provider with their content management guidelines and the latter implement them in their system.

Rightholders can configure their rules by playing on various parameters such as the duration of a recognised excerpt, for instance in perspective with the total duration of said work, or the level of confidentiality of shared content (public or private).

In the case of the threshold, in terms of duration, beyond which a rule must apply, three factors may play a part. First of all, there exists a technical threshold defined as the minimum duration of an excerpt in order to be recognised by the fingerprinting system. With technical progress, this technical threshold, which previously exceeded 30 seconds, is gradually decreasing and can sometimes be reduced to a few seconds today<sup>15</sup>.

The second is the basic threshold imposed by the owner of a content recognition system on most of the rightholders using it. This basic threshold can be for example 30 seconds or one minute by default, in order to avoid too many matches resulting from short excerpts, trailers, etc. At the request of certain rightholders insistent that very short content items should also be identifiable, this basic threshold can sometimes be adjusted downwards.

Lastly, the usual threshold is that used on a daily basis by each rightholder for their content. For cinematographic content, for example, this threshold can be set between three and five minutes, meaning that only excerpts of a longer duration will be subject to claims. This usual threshold may be adjusted by beneficiaries as they see fit for their respective content (provided it is no lower than the threshold granted to them). Of course, the more flexible a content recognition solution is in defining these different thresholds, the more its use is likely to be appropriately adaptable to rightholders' needs.

On a social network such as Facebook, rightholders can also define specific rules in the CMS depending on whether content is shared on a “wall” (i.e. on a personal space), in a group, or on a community page.

Lastly, a rule can vary depending on the location of the Internet user wishing to access the content: for instance, the decision can be made to block content only in the countries where the rightholder's commercial operation contract applies.

In general, rightholders can define multiple overlapping or complementary rules for the same content. A documentary producer can for instance decide, for one of its titles, to monetise all excerpts in North

---

<sup>15</sup> For example, Audible Magic offers three different detection thresholds of 20, 10 and 5 seconds.

American countries and, in the other territories, to block by default all excerpts of more than five minutes and manually review excerpts shorter than this duration.

Some tools are equipped with functions to detect any inconsistencies between the rules set by the rightholders. In this case, the tool alerts the rightholder on the need to put an end to the inconsistency. In other cases, the tool automatically chooses to apply the strictest rule.

The inclusion of certain platform users on white lists may also be carried out at the platform's initiative or by rightholders, most often for the benefit of the media or users of great renown or good reputation. The rightholders or platforms therefore trust them enough to exempt them from the automated control of the content they put online.

In short, the practicality of a content recognition system can now be measured by analysing these basic functionalities, namely the ability to block, monetize or monitor content according to multiple and cumulative criteria of different kinds: temporal (duration of extracts or proportion of works reproduced), geographical (at least by country), qualitative (public or private content) or personal (depending on the identity or profile of users who share the content).

➤ However, there are still some limits regarding practicality

Some features are not currently offered by online content-sharing service providers' tools. This is the case, for example, with the ability to establish rules in advance, setting an activation or expiry date. The possibility of replacing an unofficial video (e.g. a music clip) with its official version, the possibility of sending an alert notification to a third-party service in the event of a match with a fingerprint or the possibility of running a *watermark* search on a video are also not offered by default by the current CMS.

Similarly, rule design generally does not take into account the following features:

- the option to prohibit content monetisation,
- the option to share the advertising revenues with the user having posted content online (rather than everything going to the rightholder(s)),
- the option to only allow a content to play in exchange for monetisation (rather than requiring only payment of advertising revenue when such revenue is earned),
- the option to determine separate rules depending on whether the parts of the works identified are continuous or disjointed within a content uploaded on a sharing platform, or whether they are general public content versus content subject to age restrictions.

From as early as 2008, Movielabs<sup>16</sup> inventoried most of these criteria to come up with its Content Recognition Rules (CRR), a standardised model that would allow for a common language for the rules defined by rightholders regarding the automatic recognition of audiovisual content on digital

---

<sup>16</sup> Movielabs is a non-profit organisation founded by the major US film studios to advance research and development in the distribution and protection of audiovisual content.

platforms<sup>17</sup>. These rules, defined more than a decade ago, remain to a large extent relevant. However, the platforms appear to have preferred to develop their own models rather than follow the proposed standard.

The integration of new functionalities within content recognition tools helps to make them more efficient and more adapted to rightholders' needs. This evolution process is continuous and calls for a regular monitoring in order to be properly assessed.

*1.2.3.3. - In order to be both effective and practical, tools also need to be equipped with functionalities that apply following content detection.*

➤ The types of response possible in the event of detection

Once the fingerprints of protected works have been incorporated into the reference bases and, furthermore, the rules of use have been defined by the rightholders, the systems can function.

Whenever there is a match between the analysed content and one or more protected works, the automatic rules apply – to the extent possible and in accordance with the detection thresholds in effect.

The upload of a content on a given platform may trigger the application of multiple rules concurrently, for instance, if the said content includes excerpts from different works. In such cases of multiple matches, depending on the platforms, the applicable rule is that of the first identified work or the most restrictive rule out of all those possible.

In this regard, it should be noted that some recognition tools are only able to detect or process one match per analysed content item, which obviously creates problems when the content in question contains excerpts from multiple works that are supposed to be monetised on behalf of their respective owners.

Furthermore, on certain platforms, when no rule has been issued or when the system is not sure of itself (for example, if the recognition certainty rate is too low), the content identified as potentially problematic must be processed manually.

In the case of interfaces developed by digital platforms, it is in the CMS that suspicious occurrences are brought to the rightholders' attention. They – or their representatives – must then manually review each report within a given time period, otherwise the potential claim will be lifted.

For content recognition solutions that operate externally, i.e. that are not integrated into digital platforms, the service provider sends infringement notification to the relevant platforms to have the disputed content removed.

---

<sup>17</sup> Presentation and documentation about Content Recognition Rules: <https://movielabs.com/CRR/index.html>

- Follow up in the event of the detection of a protected work within a content uploaded by a user.

When content posted to a platform has triggered an automatic or manual blocking or monetisation measure, the user having posted the content is generally informed of the reasons for these measures and of the possibility to file a complaint *via* a form.

Furthermore, in the event of a match involving a musical content item on Content ID, the user having shared the content is invited to either mute the sound or delete the sound and image for the excerpt in question. In some cases, the user may also replace the contested soundtrack with music provided by YouTube. Rightholders' claims are waived when users adopt such measures.

In case users prefer to oppose a claim, complaints (or counterclaims) and any additional information are either reported to the rightholders or their representatives (that is the case with YouTube and Facebook), or processed directly by the moderators on certain platforms (such as Dailymotion). They can either accept the complaint and withdraw the claim or, on the contrary, confirm the initial decision in order to maintain the blocking or monetisation in force. According to the rules provided for by the DMCA<sup>18</sup> applied by certain platforms, if the rightholder fails to respond to the complaint, the content is made available again on the platform.

The contestation management and tracking interfaces are most often integrated into the platforms' CMS themselves, when the latter have developed their own content recognition system.

#### *1.2.3.4. –The importance of the sharpness of detection.*

Recognition by fingerprinting thus operates first and foremost according to a technical logic yielding binary results, sometimes very far from the detailed assessments that the benefit of copyright exceptions requires, on a case-by-case basis.

The stakes on these issues will require in the future to determine whether it is possible, and if so under what conditions, to set up automated procedures that would rely more on algorithms and would enable finer granularity in the analysis of each situation ("smart filtering").

However, to date, it is primarily by observing how rightholders use the practical functionalities made available to them by the content recognition systems that the sharpness of a tool can be assessed.

- Excerpt processing procedures

In practice, only short excerpts, which duration falls under the technical threshold for detecting content recognition technologies or the threshold set by rightholders, are not subject to automatic blocking or monetisation.

---

<sup>18</sup> Digital Millennium Copyright Act.

But the main content recognition technologies on the market can in particular determine the duration (cumulative or continuous) of excerpts detected automatically in analysed content, or even, for the most complete, the percentage or proportion accounted for by the excerpts detected within the whole content posted online by a user.

This means that it is possible to establish whether a match with a reference fingerprint concerns, for example short excerpts from a television programme integrated in the middle of a personal one-and-a-half-hour video; or if it is the replay of an entire passage of a work; or even a four-minute excerpt within a five-minute video (which could be the full duration of a sketch or a short programme).

The issue of quotes is not a technical one but needs legal appreciation on a case-by-case basis and it is up to the rightholders to respond to any complaints by users on these issues.

The development of these technologies could aim at supplementing the information to better grasp contextual elements needed to assess each situation or even to identify a plurality of works within a single content and thus facilitate, for example, the identification of “*mash-ups*”, i.e. mixtures of different sounds and images for creative or review purposes.

### ➤ Handling parodies

Many parodies are made by modifying or replacing the original soundtrack of an audiovisual content or by placing an audio recording from a work on alternative or intentionally misaligned images from another source.

Thus, when only the audio or the video signal of an original work is recognised and that signal appears to be associated with third-party content, it could be a parody.

Content recognition tools based on digital fingerprinting should – in theory – be able to detect such cases, as long as they have the audio and video fingerprints of the work in question.

Yet in reality, the technology can do little more than point out this possibility of a parody. Human verification is then essential to analyse the reported content and determine whether it is indeed of parodic nature.

However, in the case of cinematographic works, it is also important to recall that the same film will have multiple soundtracks due to dubbing in different languages. But each language version of the same film does not necessarily have a separate specific audio digital fingerprint. A video whose audio track differs from the original version is thus not necessarily a pastiche or a diversion ; it may simply be a foreign version of the original content.

Lastly, in practice, many content recognition technologies are specialised in either audio or video. As a result, audio and video fingerprints are still mostly the result of different technologies, possibly offered by different providers, *via* different procedures. This does not facilitate the comparative and simultaneous analysis of the soundtrack and the image from a video.

This fragmented technological landscape, combined with the non-exhaustive nature of fingerprint reference bases, make it very difficult in practice to automatically identify pastiches or parodies.



Only the existence of “multimedia” system (covering both audio and video fingerprints) and “multilingual” system (i.e. accepting more than one audio fingerprint for the same video content) would be able to help detect possible parodies automatically. However, as it has been pointed out, manual and human validation would still be necessary to correctly identify a parody. Thus, at the present time, technology alone is clearly not able to respond to the need for automated processing of parodies.

### 1.3. - Current avenues for development do not call into question the central role of fingerprint-based technologies.

While fingerprinting appears to be the most widely used and most reliable technique, new technologies could come into the picture, improving and complementing existing content recognition systems, particularly in cases where, to date, there might not be a digital fingerprint for each content unit requiring protection.

These are: first, artificial intelligence, which can improve the performance of existing recognition tools, generally speaking and subject to certain conditions; and, second, algorithms which, although currently used for functions other than copyright protection, could be used alongside existing solutions. However, care should be taken to ensure that these innovative uses fully comply with the rules on respect for individual freedoms<sup>19</sup>.

#### 1.3.1. - Artificial intelligence and content protection.

In the following brief lines, we will present the principles underpinning artificial intelligence and deep learning<sup>20</sup>. The recent advances in artificial intelligence are radically reshaping the techniques implemented and appear set to achieve unprecedented quality of performance. However, these new approaches come with many limitations of their own. It is thus important to keep in mind that artificial intelligence is not the silver bullet for any problem, even though this attractive concept is currently very often promoted in commercial communications strategies by many technology solution providers.

In the field of content analysis, artificial learning can be used to enable computers, drawing on analysis of vast datasets, to perform a wide variety of tasks, from image recognition to segmentation (separating an object from the background), facial recognition, annotation propagation, classification, content recommendation and voice recognition. In essence, it operates by putting to work

---

<sup>19</sup> The following description of technologies and uses, for prospective purposes, should by no means be construed as a recommendation on the part of the mission regarding their implementation. In many respects, the privacy issues which they are likely to raise rather emphasise the advantages, seen from this perspective, of the other recognition methods described above, and in particular those based on the fingerprints placed on protected content.

<sup>20</sup>For more detailed analysis, see the courses given by Yann Le Cun at the Collège de France.

mathematical and statistical approaches to give computers a certain ability to learn how to solve these tasks, even without the computer being explicitly programmed to do so.

Although effective, artificial intelligence must be run under supervision, in order to be certain that content is being recognised effectively.

For instance, a programme must be fed with thousands or even millions of qualified examples before it learns a model that best describes what is provided to it. It is because a supervised learning algorithm is fed with thousands of images of cats, dogs, planes, etc. that it “learns” to recognise that it is dealing with cats, dogs and aeroplanes.

More precisely, the programme learns to determine a good fingerprint to represent these concepts but also how to separate the different categories that will have been shown to it. The learning process has generalisation capabilities, that is, it can to some extent recognise an object which it has never seen before, provided there is some similarity between what it is given and what was used for training.

The use of supervised artificial intelligence to process multimedia can enable never-before-seen success rates, but with two major drawbacks.

First of all, the technique works most effectively when dealing with contemporary content, as systems are most often “taught” using millions of contemporary references. In the field of image, for example, recognising animals in medieval illuminations when the concepts for such animals were learned from modern photographs proves too much to ask of the technology. Likewise, it is not very effective at learning from only a small range of examples, or at learning on the fly.

Secondly, any form of automated learning requires considerable resources. Not only is it necessary to create a very large mass of annotated data, which can be costly to produce; it is also essential to have access to expensive computing resources and great deal of time. It sometimes takes thousands of hours of calculation to process millions of examples or to “relearn” periodically based on new data.

Lastly, there are doubts about the reliability of the results obtained.

While the fingerprint systems created by the researchers and the related recognition methods are perfectly clear and entirely reproducible and controllable, the results produced by artificial intelligence can prove quite obscure.

The scientific community is not always able to guarantee the complete reliability of the results produced by artificial intelligence. Although they are generally very good, they can sometimes contain unexpected errors which researchers have trouble explaining.

For example, it has been shown that it is very easy to trip up an artificial intelligence when a specific disruption, invisible to humans, is introduced into an image. Conversely, it has been shown that it is difficult to trick an image recognition systems based on traditional fingerprinting techniques, such as those described previously in this report<sup>21</sup>.

---

<sup>21</sup> See the work by Thanh-Toan Do, researcher at the University of Liverpool: [http://www.irisa.fr/texmex/publications/Author/Thanh-Toan.Do\\_fr.php](http://www.irisa.fr/texmex/publications/Author/Thanh-Toan.Do_fr.php)

### Illustration of possible decoys for AI-based recognition algorithms

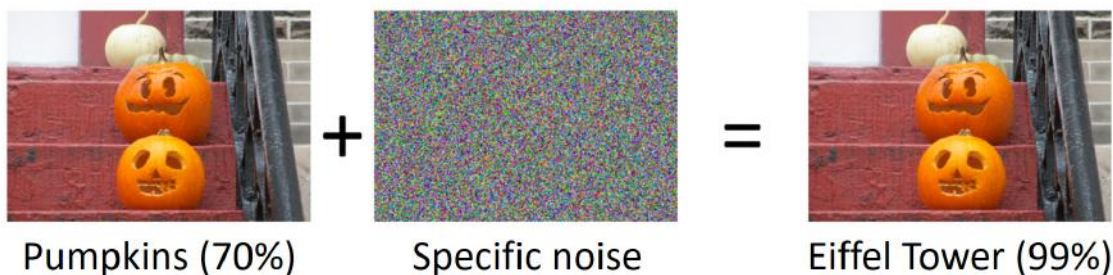


Figure 12

Artificial intelligence has no trouble recognising the image on the left as one containing pumpkins. The recognition confidence level is quite good, at 70%. However, when a very particular type of disruption which we might perceive as visual noise (middle image) is added to the pumpkin image, artificial intelligence is completely thrown off-track, and identifies something entirely different in the image, namely the Eiffel Tower, what's more, with complete confidence. This surprising but true-to-life example shows that it is possible to pass one piece of visual content off for another without it being noticeable to the human eye. Artificial intelligence can thus be lured into asserting that content the author of which is X will be perceived as content produced by Y and thus mistakenly monetise it. It may also accept something for what it is not (for example, child pornography content as something innocuous, within a parental filter). This area of research is referred to as *adversarial machine learning*.

Source: Hadopi and CNRS-IRISA (L. Amsaleg)

Where content recognition on digital platforms is concerned, proficiency in the techniques of so-called "*adversarial machine learning*" could be used to pass protected or prohibited content off for innocuous content, or even to pass protected content off for other content (and thus unduly receive any remuneration resulting from it).

It is thus important to remain cautious about the opportunities opened up by artificial intelligence, so long as extensive experimentation has not demonstrated its effectiveness.

In summary, artificial intelligence promises unparalleled efficiency, but requires huge datasets for training. It also requires computing infrastructures that are cumbersome, complex and costly to implement. Above all, for the time being, it continues to be fraught with reliability, security and trust issues. Methods for misleading it have been identified, but not those for guaranteeing its reliability.

It nonetheless remains that artificial intelligence is useful. Some of the practical applications discussed below, for instance, have seen their performance increase tenfold thanks to the technology. It is simply a matter of being aware of its limits at the same time.

1.3.2. - Content analysis solutions used today for purposes other than copyright protection.

*1.3.2.1. - Solutions already used for filtering inappropriate content.*

The major digital platforms already use solutions to filter content put online by their users, but for purposes other than recognising content protected under copyright or related rights.

Platforms such as Facebook, YouTube and Instagram use filters to detect any content that might be in breach of the general terms and conditions of use set out for their services, particularly with regard to nudity and violent content. Since November 2019, YouTube has also been using a machine learning solution to identify content uploaded by users and which is clearly intended for children, in accordance with the US Children's Online Privacy Protection Act (COPPA).

Other tools are already being used by platforms, such as emblem recognition in image content. For instance, an algorithm can recognise the emblem of a terrorist organisation on an image or video, especially when it appears in a corner of the image, and raise an alert so that the flagged content can be subject to more specific analysis.

Instagram is currently testing tools to detect whether a comment by a user is offensive, inappropriate or contrary to the platform's rules of good conduct.

Should any doubts remain, an alert is issued informing the user of the potentially undesirable nature of his or her comment and requests confirmation of the user's continued intent to post it.

Since 2016, social media have also used algorithms to detect suspicious behaviour, through automated inspection and cross-checking of large amounts of information about users. The challenge here is to be able to identify fake user accounts that are actually controlled by bots with the aim of spreading false information or manipulating public opinion, particularly during elections. Facebook reports that it automatically deleted between 600 and 800 million fake accounts per quarter in 2018.

On the same principle, the study of data from content recognition tools could - while remaining in compliance with data protection rules - enable any platforms so desiring to better identify suspicious users or, to the contrary, conduct likely to be based on good faith.

Solutions based on taking into account the profile of users subject to blocking or monetisation measures could also be considered. Depending on a user's profile (official or non-official account), on their history and the possible existence of incidents in the past, on the usual number of consultations of the content posted by that user, etc. algorithms could present to rightholders, as a priority, the most critical cases of content containing their works and for which manual review is necessary. The same applies to the handling of disputes raised by users following automatic or manually-entered claims: depending on the context, some disputes require more urgent responses than others and algorithms could help to manage them better. This type of intelligent sorting (or smart filtering) of fingerprint matches, or of disputes filed by users, may considerably facilitate rightholders' tasks, in particular if the latter can participate in a productive manner, from the beginning, to the development of such algorithms.

Lastly, machine learning is already in wide use by the social media and could be used to improve the categorisation of content shared by Internet users.

The basic principle consists of creating large databases of videos corresponding to a specific type of content (for example, today, pornographic content). Algorithms then analyse all the content gathered in the database and become familiar with the similarities found between the content items. The more content the database contains and the more qualified and divided into categories and sub-categories it is, the more accurately the algorithm is able to guess the nature of an item submitted to it for analysis. As explained in the previous point, the size of the qualified database is critical because, unlike a human brain that can quickly recognise a cat after seeing only a few examples in photos, artificial intelligence algorithms function differently: it is the number of examples provided to the programme that makes up for the system's lack of "common sense" and intuition.

Side effects and false positives are quite common because, in contrast to fingerprinting technologies, which are aimed at identifying very specific content, *machine learning* tools are designed to be able to interpret the nature of content encountered for the first time. The existence of a margin of error is inherent in the concept of *machine learning*, and the aim for developers of these tools is to minimise this margin of error as much as possible. False positives can also be incorporated as such into the qualified base in order to help the algorithm better distinguish between what needs to be recognised and what does not. The learning process is thus continuous.

By creating significant databases of examples of fictions, music videos, sports programmes, personal videos, trailers, etc., it is conceivable that a machine learning algorithm will be able to gain a fairly precise idea of the nature of the content which it is asked to analyse, without any need for "traditional" digital fingerprinting, as offered by Content ID or Audible Magic. The goal here is not to recognise an artwork in particular but to understand what the type of an analysed content is.

For example, a sporting event broadcast has very specific characteristics, entirely distinct from other types of content and even very distinct from one sport to the next (football, tennis, skiing, boxing, etc.). By going through the video streams broadcast live on a given digital platform, an algorithm can thus quite easily isolate the streams likely to be those of sports competitions, whether the said algorithm is incorporated into the platform or operates from outside. This solution can even work when the title of some of these live streams is misleading or gives no relevant information about its actual nature.

### *1.3.2.2. - Automatic speech-to-text recognition.*

Automatic speech recognition is a solution already widely in use on YouTube. This practice, also known as *speech-to-text*, consists of automatically transcribing what is heard in an audio stream or on the audio track of a video into raw text.

For the time being, this technique is used to automatically generate the subtitles of a video.

The text generated automatically by the platform can be used for many purposes: analysing the text transcribed with the aim of offering targeted contextual advertising (or possibly with the aim of

preventing the monetisation of videos dealing with subjects considered sensitive), detecting hate speech, violent messages or content contrary to the conditions of use of the service, etc.

This technology could also be used to recognise works, by comparing the automatically transcribed text with databases of scripts, books or texts subject to copyright in order to find possible matches. It could thus become possible to recognise any content of a book or dialogues from a movie.

It should be noted that the error rate when transcribing certain sound recordings is substantial, especially when there is background noise, as the latter can make it complicated to properly understand the words. However, once a certain quantity of text has been recognised with a satisfactory degree of quality, it is nonetheless possible to state whether this text matches the works found in a reference base to any significant extent.

#### *1.3.2.3. - Optical Character Recognition (OCR).*

Optical character recognition has long applied to digitised documents or still images. OCR makes it possible to recognise the text visible on these optical media, then convert this text into raw form so that it can be easily handled and modified.

Multifunctional platforms dedicated to the analysis of audiovisual content, developed today by large corporations such as Microsoft (Video Indexer) or Google (Cloud Vision) and including tools linked to artificial intelligence, already offer OCR modules applied to video. The purpose of these modules is to transcribe into plain text all readable inscriptions that might appear in a video, whether they are titles, subtitles or even moving and dynamic inscriptions visible in a filmed setting (poster, information panel, etc.).

This type of technology can be useful in detecting the graphic representation of protected text in a video, such as song lyrics in music clips or karaoke videos. This technique can also be used to detect filmed reproductions of comics, manga or webtoons (comics intended to be viewed on digital terminals), as texts or speech bubbles commonly appear on these types of works.

Once a sufficient amount of text has been recognised with a good level of trust, it is possible to compare the identified text with a database of protected texts or song lyrics to look for possible similarities.

The addition of OCR functionalities to multimedia content-sharing platforms could thus make it possible to provide a response to the needs voiced by some publishers of protected content, which for the time being have remained unaddressed.

#### *1.3.2.4. - Logo or trademark recognition.*

This technique consists of searching within still or animated images for specific symbols (or markers), logos or registered trademarks. In a sense, logo or trademark recognition is an evolution of the OCR technique (which remains limited to text recognition).

Automated logo or trademark recognition can have many uses.

The technique is already used on certain platforms and by certain specialised services to monitor propaganda content spread by terrorist groups, accustomed for years to displaying the emblem or flag of their organisation in their images.

Television channels or sports leagues, which often display their logo on screen in various forms, may also have an interest in encouraging the development of logo recognition tools for the purpose of detecting and verifying content with their images or visual identity, including when the logo appears only in passing, in a stadium on the edge of the playing pitch. This makes it possible to identify proprietary content for which no digital fingerprint has been made beforehand.

With regard to the holders of registered trademarks, this technique can also be used to detect depictions of products bearing their trademarks, which may be useful in the fight against counterfeiting.

Logo or trademark recognition is more a more flexible technique than traditional digital watermarking because it allows, with much more tolerance, recognition of the representation of a distinctive shape (logo or mark). Moreover, unlike digital watermarking, this technique does not require the prior marking of content in order to work: the targeted pattern need only be visible in the image for recognition to be possible.

In contrast, this solution is quite fragile: if a logo appears as a still image in the corner of a video, all it takes to trick the detection tool is to reframe the image so that the logo can no longer be seen.

Logo or trademark recognition also cannot, in theory, be used to recognise a particular work. It is furthermore likely to return a large number of matches, which will then need to be sorted and checked manually.

#### *1.3.2.5. - Facial or character recognition.*

Facial recognition systems have been in existence since the 1960s and are already widely used on certain digital platforms, such as Facebook. These tools are also deployed in certain public video surveillance systems. They are also found in the operating systems of most modern smartphones, where they are used to facilitate automated photograph sorting.

It is said that these systems could be used for video content recognition, as well, by analysing the faces of the actors. Once a sufficient number of actors have been identified, the audiovisual work in question can be determined by elimination and with a good degree of confidence. From a statistical point of view, there are very few audiovisual works in which the same four or five distinct performers can be found.

This method is implemented by connecting an algorithm firstly to a database of celebrity photos (such as the “MS Celeb” database created in 2016 by Microsoft) and secondly to another database containing details about films and TV series casts (e.g. iMDB or Allociné).

The current systems such as Microsoft's Video Indexer are also able to record the frequency with which a character appears on the screen as well as its total duration of presence in a video, which makes it possible to refine the analyses.

The same process can be used to guess which teams are playing in an excerpt of a sports match, by attempting to recognise each of the players seen on screen.

This technique currently needs relatively little computing power to operate and can be used on live broadcast images. The ability to accurately recognise individuals is quite high for film and television images, where characters regularly appear in close-up and with optimised lighting, compared to the results achieved, for example, when studying video surveillance images taken in public spaces. The number of false positives sometimes seen with this form of biometric technology can thus be kept to a minimum.

The use of facial recognition systems, however, raises legitimate questions about privacy and personal data, especially if such use were to become widespread. It thus requires special regulation.

Lastly, in September 2019, Microsoft launched a tool capable of recognising fictional characters from comics, animated features or computer-generated images. Character recognition technology can thus now be applied to the world of drawing and animation and be considered for content from interactive works such as video games or virtual reality, which are usually not very compatible with traditional digital fingerprinting systems.

#### *1.3.2.6. - Key images detection and computer vision.*

Key image detection and computer vision are relatively recent techniques, but made significant progress in the late 2010s. These tools are becoming increasingly powerful and sophisticated and can now be used for large-scale projects.

The detection of key images, first of all, consists of identifying the most relevant images in a video, likely to be used for more detailed analyses. The task consists of eliminating redundant images as well as blurred or useless images (black screens, etc.). This preparatory stage simplifies the analysis work that will follow.

Then comes the computer-assisted vision stage. Modular tools, such as Google's Vision AI or Microsoft's Computer Vision, attempt to recognise specific objects or locations on the images provided to them. To do this, the tools work with databases which are themselves created using *machine learning* techniques. They thus try to identify each of the elements found in the image (this can be a person, an animal, a characteristic utensil, a famous monument, etc.) and assign each an estimated degree of reliability.

The latest algorithms can even automatically draft a description proposal such as “a football player on a playing field – 96% sure”, “Tom Cruise in a suit and tie standing in front of a building – 97% sure” or “a group of people sitting in front of Güell Park in Barcelona – 53% sure” to describe an image submitted to them. Other tools, such as the ones used by Facebook and Instagram, attempt to define



the mood of the people in the images according to predefined categories: laughter, fear, anger, sadness, etc.

Linked with existing registers of scenarios or synopses of audiovisual works, these tools will eventually be able to associate the description of video content with the summary of an audiovisual work, obviously in a more or less certain manner depending on the case at hand. However, it sometimes takes only a few elements to reduce the range of possibilities to a handful of films (for example: a meadow, Cary Grant, a plane flying in the same scene).

While computer vision tools continue to make mistakes regularly, their capabilities are improving and their potential remains quite considerable. Companies like Marklogic are already working with major film studios to mass-produce metadata from video catalogues and through artificial intelligence. The data resulting from this work is then used to archive and reference content as well as for advertising or legal purposes.

The artificial intelligence research centres of a number of large Internet companies, several of which are located in France, continue to work on these emerging areas. One of the challenges for the future of computer vision solutions is the computing power needed to analyse the images, hence the fact that most solutions today rely on cloud computing in order to operate at the required speed.

### 1.3.3. - Longer-term avenues for development

In the longer term, it is expected that technical progress, combined with the continued aggregation of content recognition tools with one another, will make it possible to offer far more effective solutions for managing and recognising works protected by copyright and related rights.

Independent research laboratories, just like the Internet giants, are already experimenting with these solutions.

#### *1.3.3.1. - Detailed action description (“story analysis”).*

Today’s computer vision tools are able to describe the content of an image, but have trouble describing and interpreting actions or intentions.

In the future, once the different pieces of software have been combined and improved, computer-assisted vision tools should be able to better understand situations. Already, some algorithms are able to detect unusual or suspicious behaviour in public places, based on CCTV footage.

Studying the way in which actions develop, key image after key image, will thus make it possible to depict how a scene unfolds. The contribution of other modules tasked with listening to and understanding the words of various protagonists will further enrich this understanding of the stories. The practice of describing the plot of an audiovisual content item has been dubbed “story analysis” by some experts.

This analysis method will make it easier to identify any match between a reviewed video and the summary, synopsis or script of a protected work (i.e. the reference). The same method could also be

used to directly detect offensive, violent or inappropriate content being distributed on digital platforms and alert moderators, or suspend the content in question as early as possible, when in doubt.

### *1.3.3.2. - Similarity-based content search and plagiarism detection.*

In the publishing sector, significant and noticeable progress is expected in technologies enabling comparison between articles or documents.

A number of solutions, such as Copyleaks, PaperRater and Turnitin, already claim to be partially powered by artificial intelligence technologies. Solutions of this type are capable of detecting characteristic similarities between different texts, including when a text has been copied then translated into another language.

Moreover, with the growing need to detect differences between multiple seemingly similar texts, particularly in order to better identify fake news and information manipulation on social media, new methods of comparative analysis will develop. These will offer both greater refinement and flexibility than current tools.

It is thus believed that they will not only be able to more effectively identify unauthorised redistributions of protected texts, but also reappropriations or plagiarism.

### *1.3.3.3. - Multiformat searches (video versus text, etc.).*

The current content recognition methods continue to work in a fairly hermetic manner, by content type: audio fingerprints are compared with other audio fingerprints, images with other images, etc.

This relatively compartmentalised operation is expected to eventually fade out, giving way to multi-format content recognition, in other words, between different types of media.

In the case of audiovisual and text, an algorithm tasked with analysing a film will, for example, be able to recognise that it is the adaptation of a book. Similarly, it will be possible to detect when a journalist's investigation published in a newspaper, is in fact largely taken from a pre-existing television documentary. It could even be that recognition tools will someday be able to detect when a Japanese comic is telling the same story as a French musical.

However, it will take time before the various technical solutions needed can come together and form a coherent whole, and for the related reference bases to come about and interconnect.

## 2. - Stakeholder perceptions and expectations: content recognition tools at the crossroads of the visions and interests of platforms, rightholders and users.

To analyse the expectations regarding recognition tools today, at least three categories of actors must first be distinguished:

- The platforms, which played the predominant part in determining the operating procedures and scope of implementation;
- Rightholders for whom certain recognition tools have been set up, when access to recognition tools varies greatly from one sector to another;
- Users, understood mainly in the sense of people uploading content to platforms, with a special place for videographers (or “YouTubers”) whose aim is to generate revenue from their content production activity.

The respective conceptions and interests with regard to recognition tools as presented in the first part of the report do not converge, whether between or within these three categories.

2.1. – Thus far, the platforms have focused on becoming proficient in deploying content recognition tools, regarding both their concepts and their scope and methods of implementation.

Online content-sharing service providers implemented recognition tools in a context where they considered themselves not obliged to do so because of their status as simple hosts. As a result, they presented these recognition tools as arising from a voluntary initiative on their part. However, insofar as the level of protection provided for the various types of content on the platforms varied, this voluntary approach by the platforms was clearly adopted to ensure a more favourable balance of power with the rightholders.

2.1.1. - Audio and video sharing platforms: content recognition was first deployed on a large scale by YouTube, which determined its functionalities and uses.

2.1.1.1. - Content ID was deployed in a context of litigation with certain rightholders who were dissatisfied with both the performance and the complexity inherent in the take-down request procedures.

Whether in the United States or in the European Union, for a long time, the presence of illegal content could only be countered by using the official removal procedure, otherwise known as the "notice and take-down" procedure, linked to the host providers' status of platforms.

#### **The host provider's status**

*Directive 2000/31/EC of 8 June 2000, transposed in France by Act No. 2004-575 of 21 June 2004 on confidence in the digital economy (known as LCEN), introduced the concept of hosting provider and associated this concept with a limited liability regime with regard to stored content. It stipulates that the hosting provider is not likely to be held liable in this respect if it:*

- *is not aware of the illegality of this content;*
- *or acts expeditiously to remove this information or disable the access to it upon obtaining knowledge of its illegality.*

*Article 6-1 of the LCEN provides that the hosting provider's knowledge of the disputed facts is presumed to have been established where notification of unlawful content has been received.*

*Like the American model resulting from the DMCA (Digital Millennium Copyright Act), the notification procedure for unlawful content provided for by the LCEN requires that the unlawful content be described and that its location on the site be precisely stated. The take down request covers only the location of content indicated in the notification, although this content may be present or accessible from multiple places on the site.*

*In addition, the unlawful content reported and removed may reappear as soon as it is made available by a web user, thus making the notification unending. While the Court of Cassation, in rulings of the 1<sup>st</sup> civil chamber of 12 July 2012, refused to make the absence of liability conditional on measures preventing the online re-uploading of previously reported manifestly illegal content (notion of "stay down"), the Court of Justice, in the recent Facebook Ireland ruling<sup>22</sup>, introduced, with the notion of "equivalent information", an opening in this sense.*

---

<sup>22</sup> Judgement handed down on 3 October 2019 by the Court of Justice of the European Union under no. C-18/18 in case *Eva Glawischnig-Piesczek v/ Facebook Ireland Ltd*: the Court finds that the prohibition on imposing a general monitoring obligation on a hosting provider does not preclude it from "ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the

*In any case, the burdensome notification procedure, which must be implemented for each illegal content identified on a platform, explains the importance, for effective protection of copyright and related rights, of a process for monitoring content uploaded by a digital fingerprint system.*

The very restrictive notification procedure has therefore prompted the most important rightholders in the United States to ask the main sharing platform, YouTube, to find more practical solutions, in line with the exponential growth in the volume of shared content. Dailymotion played a pioneering role in the deployment of a technology-based fingerprinting solution from Audible Magic (for sound) and the French National Audiovisual Institute (Signature, for video). Google, taking care to present its approach as purely voluntary, albeit against a backdrop of litigation and negotiated settlements with some rightholders, then set up its own tool, Content ID.

Addressing both the massification of sharing practices and the problem of illegal content reappearing after removal, recognition tools make it possible to block *a priori* the sharing of unauthorised content. They are dependent on close cooperation between the platforms and the rightholders to whom they open the benefits. They involve the provision, by rightholders, of either digital files containing the protected content or fingerprints: as much as the performance of the recognition technology, it is the depth and breadth of the fingerprint base that makes it effective.

YouTube has thus made its tool the standard, by virtue of its long-standing presence (on the Internet scale), the sophistication of the management functions it offers and the depth and breadth of the content base it protects.

#### *2.1.1.2.- A tool shaped by YouTube's expectations and interests.*

The deployment of recognition tools has helped to pacify the relationship between rightholders and the Google platform. Once often viewed with suspicion, Google's platform is now a major player in content distribution, with the rightholders concerned by Content ID also seeing it as a partner in the implementation of their rights<sup>23</sup>. However, the deployment of recognition tools continues to be shaped by three challenges for YouTube:

- A legal certainty challenge: recognition tools have essentially been deployed with a view to gaining legal security for the platform. By pacifying its relations with the rightholders whose content is shared, and particularly the most influential, its aim was to perpetuate its business model, and thus ensure attractiveness for its advertisers;

---

monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content" (Nr 53).

<sup>23</sup> According to the *How Google fights piracy* 2018 report, 98% of YouTube copyright and neighbouring rights claims in 2017 were processed using Content ID (rather than the notification and take-down process). In more than 90% of the cases, the beneficiary chose monetisation.

- This is a central challenge for the smooth operation of the platform, which rests on the ability for users to immediately share a volume of content that precludes *a priori* human control (some 500 hours of new videos shared each minute). In the same spirit, having complete control over the tool, Google can optimise its integration into the platform, by ideally set the necessary calculation capacities.
- Another aim was to find a positioning that would make the platform a third party player in the event of disputes between rightholders and users. The attachment in principle to the host provider's status aligns here with the platform's resource efficiency principles. The platform therefore makes it clear that, should a dispute arise, it would be limited to providing the parties with the dialogue tools needed to manage disputes. This does not preclude the fact that, in reality, the choices it makes in defining these tools decisively shape users' practices, and that, in the event of dispute among with a user over a removal or a block, it takes decisions on the admissibility of counter-notices<sup>24</sup>.

In view of these statements, the platform thus defines the tools available to rightholders and chooses the rightholders to which they are open as well as the concrete opportunities it offers them in managing their rights. Access to the different "levels" of Content ID, which offer different degrees of acuity in managing rights and conflicts, is determined by the platform's policy: given the significant powers granted to the rightholder thanks to the rights management tool at its highest level, the platform wishes to reserve it for the rightholders who have the largest catalogues, while defining for the other partners simplified tools or offering less latitude in managing rights, thus inevitably stirring requests from those of the rightholders who are less well treated<sup>25</sup>, and in some instances even political concerns about the resulting differences in treatment<sup>26</sup>.

### *2.1.1.3. - The changes made to the tool over time reflect a cooperative dynamic between YouTube and the rightholders using the platform.*

Recognition tools are governed by a law of constant improvement and fine-tuning: the platforms have, when they are the creators of their own tools, adapted to their needs and constraints, have shaped

---

<sup>24</sup> Again according to the report *How Google fights piracy*: in addition to the fact that (p. 24) 98% of Content ID copyright claims on content shared on YouTube in 2017 were processed automatically (automatic identification by Content ID and automated application of the rule defined by the beneficiary), YouTube itself carries out a review of any online requests made by users, when these requests relate to a takedown notice sent manually by a rightholder (page 31). With regard to these counter-notifications (a request by the user to remove a block or take-down), YouTube received 150,000 of them in 2017 (concerning 200,000 videos) and states that it tasked its teams with an initial examination to ensure the presence of the necessary legal elements and a valid reason for reinstating them online ("*sound rationale for reinstatement*"). On that basis, it would reject two-thirds of these itself.

<sup>25</sup> In its meeting with the Mission, IMPALA, which represents independent music producers in Europe, reported that many of its members do so.

<sup>26</sup> In a letter to Google CEO Sundar Pichai on 3 September 2019, 8 members of the U.S. Congress expressed concern about the difference in treatment in access to Content ID for holders of "smaller" catalogues, requesting a response by 30 October 2019 and convening its representatives for a Congressional round table on access to Content ID.

their development, offering a response to all the expectations of the rightholders concerned. This is particularly the case of YouTube, which set up its tools in this regard relatively early and therefore boasts fairly lengthy experience in deploying them.

The example of content broadcast live offers an effective illustration of this scalability in response to uses. With the development of live broadcasting on exclusive broadcast programme platforms (primarily sports competitions, such as football matches), recognition tools have been improved so that counterfeit content can be identified more quickly. Here too, it is the rightholders who urged to make live broadcast content identifiable, the responsiveness of the platform being particularly important in preventing the business model of exclusively broadcast content from being weakened.

Meanwhile, the platform found that the development of recognition tools proved a powerful means of ensuring that its content offer would include rightholders willing to operate under the monetisation model (which is the case for 90% of content covered by Content ID), particularly in the music field. Recognition tools must be seen as a real investment for platforms because they allow them to legally secure their offer and give access to a richer offer to users. Similarly, recognition tools give the platform the chance to better target its commercial offering for advertisers. Recognition tools thus become one of the components of the platform's economic model.

In the ever-changing world of digital uses, the recognition tools deployed by the platform therefore reflect at each moment the point of balance reached between its strategy and that of the rightholders to whom it offers its use. This balance is reflected in the functionalities offered to each category of rightholders defined by the platform, for example the parameters integrated in their interface (CMS). It is also reflected in the rules for creating fingerprints, which YouTube agrees can be made by the rightholder without the protected content itself being delivered, but in this case without giving the rightholder the latest version of its technology or ensuring the back-compatibility of the fingerprints (which have to be resubmitted). Lastly, it is reflected in the fingerprint management rules (in particular the rule that allows only one fingerprint to be generated per content item) and in the functionalities open to users who share content.

The recognition tool deployed by YouTube is therefore constantly evolving, with each of the decisions made by the platform, seeing the complex interaction between the expectations and requests of its advertisers, rightholders and users.

#### *2.1.1.4. - The other audio and video sharing platforms have been able to set up recognition tools, but these remain in some cases incomplete.*

While YouTube has a certain lead in implementing recognition tools, the other platforms for sharing audio or video content (Dailymotion, SoundCloud, Tiktok, Twitch) have also been able to implement such tools, at the request of rightholders, with DailyMotion playing a pioneering role in this area.

The main expectation of platforms in implementing recognition tools is to minimise development and deployment costs, an expectation that is all the stronger as they hold a smaller share of the advertising market than YouTube with which to finance these costs.

Nonetheless, it is not always easy to ascertain which tools these other platforms have put in place, with contradictory information sometimes even circulating as to whether they have actually deployed one. Naturally, they all, as a matter of standard procedure, take into account the concerns necessary to guarantee respect for intellectual property rights in their general terms and conditions of use<sup>27</sup>, and have been able to sign agreements with some rightholders; however, the implementation of these agreements is not always dependent on the deployment of recognition tools, since rightholders may in some cases be satisfied with an *a posteriori* analysis of uses, particularly during an experimental phase.

Generally speaking, these sharing platforms tend to highlight the size of the investments involved, which would be disproportionately high if they were expected to achieve the same level of performance in content recognition as YouTube. It was largely from this angle that they took part in the debate on Article 17 of the Directive on copyright in the Digital Single Market and participate today in the work on its implementation.

This is the case with Twitch, which initially specialised in the distribution of video game sessions, but which must, considering its success and degree of expansion, be seen as a platform for sharing different types of protected content. The main concern expressed by Twitch pertains to the cost of deploying recognition tools, which could undermine the platform's business model. In the debate on Article 17, Twitch requested:

- A clarification of those cases in which the platform should be considered under Article 17 as carrying out an act of communication to the public, Twitch arguing for the broadcasting of live content to be excluded;
- Better access to knowledge of protected rights and to rightholders, in a landscape where protected content and the rightholders concerned are very diverse, and moreover likely to change with time. For Twitch, it is as important to reflect on the formats in which information is provided by rightholders as to ensure the development of recognition tools.

## 2.1.2. - Generalist social media and other platforms have been able to deploy audio and video content recognition tools.

While online sharing platforms specialising in audio and video have naturally been the trailblazers in the deployment of recognition tools, more general social media have also been called upon to do so, as they offer the same type of sharing features. For example, although Facebook does not make the monetisation of shared content central to its business model, it nonetheless allows this content to be shared on a large scale and has therefore had to deploy a recognition tool.

---

<sup>27</sup> Maintaining accounts is generally conditional on compliance with intellectual property rights, as multiple violations may lead to account deletion.



### *2.1.2.1 - The Facebook case: a tool enabling blocking and monetisation on all shared content, but offering fewer functionalities than Content ID.*

While Facebook does not see itself as a platform for sharing audio and video content, insofar as it offers that sharing function, it has developed its own tool, Rights Manager, intended to ensure copyright protection based on fingerprinting technology and which has been extended to Instagram.

As with YouTube, the tool is also used to manage the monetisation of content, even if this monetisation is not, as Facebook itself states, central to its existence.

Rights management falls within a specific framework with Facebook/Instagram, due to the private nature of certain accounts, making it difficult for rightholders to find out about the exact use of their content. Facebook ensures the privacy of its accounts is respected when the owners so choose, such that it does not reveal the identity of a person having uploaded content protected by copyright and related rights.

Furthermore, except in exceptional instances, Facebook generally requires that rightholders provide it with the content from which the fingerprint will be generated. Facebook does not want to give the rightholder the opportunity to generate its own fingerprint.

Facebook is in the process of rolling out its tool, which for the time being, does not offer all the rights management features that YouTube's tool does.

For Facebook/Instagram, copyright protection is more broadly part of the fight against illegal content on the social media, in particular those linked to terrorism, child pornography, hate speech and violence.

### *2.1.2.2.- Other social networks, which can either largely or more occasionally be used to share protected content, do not use content recognition tools.*

Video or audio content can be shared on a variety of social media, such as Twitter, Snapchat, Dubsmash or LinkedIn.

All of the aforementioned social media specify in their general terms and conditions of use that users must respect copyright, but have not put in place any recognition tools, keeping to the standard procedure of “*notice and take down*”<sup>28</sup>.

Not having been able to review in detail the practices of these actors, for the time being, the mission notes that the presence of content protected by copyright is perceived as less central than on other sharing platforms.

---

<sup>28</sup> Twitter: <https://help.twitter.com/fr/rules-and-policies/copyright-policy>

Snapchat: <https://www.snap.com/fr-FR/terms> (point 7)

Dubsmash: <https://dubsmash.com/terms> (item 10)

Overall, platforms have deployed content recognition tools in a constant search for the right balance between attractiveness to advertisers, breadth of content for users and satisfactory balance of power with the most influential rightholders. In this context, some platforms have managed to make real efforts, in particular when, after an initial period that was sometimes experimental, even unbridled, the legal security of the business model appeared to be central, with attractiveness to advertisers and investors having the same importance as the requirements of rightholders.

However, the platforms that have deployed content recognition tools have always been careful not to appear as arbitrators between rightholders and users.

### 2.1.3. – The quest to control costs associated with content recognition for platforms and market responses.

Platforms or the representatives thereof often cite the issue of cost as an obstacle to the implementation of solutions capable of recognising protected content – at the risk, it should be said, of overlooking the revenues generated by the presence of this same content.

The cost question was in fact raised during the negotiations on Article 17 of the Directive on Copyright in the Digital Single Market and brought up again at the Stakeholder Dialogue held at the initiative of the European Commission in Brussels on 5 November.

However, considering the state of the market when it comes to recognition solutions implemented by third-party service providers, the mission advises a tempered view. While actors such as Google and Facebook have developed proprietary tools and incorporated them into their existing platforms, platforms can also call upon a number of specialised service providers. Two types of business models were brought to the attention of the mission in this regard.

In the first model, the platform can use technology against payment for a license, usually associated with a cost depending on the number of requests or volumes to be analysed. This is the case, for example, of the INA-Signature solution, whose rates, already listed in the CSPLA report of March 2017 on recognition tools, have remained on the same order of magnitude. For a video content sharing platform, video content analysis is available from €2,700 per month, for an incoming stream of 100,000 hours of content (equivalent to 600,000 requests on 10-minute videos) subject to analysis, with a response time of less than 5 minutes. The rightholders separately subscribe purchase a flat-rate service to have the fingerprints of their choice activated for analysis, at an annual cost of €5 per hour of content. Fingerprint creation and storage is free of charge.

Another service provider, the company Videntifier, also offers a monthly rate that varies according to the volume of content to be protected (the concept is known as “*reference collection size*”, in the table below) and the volumes to be verified (referred to as *daily query throughput*). Videntifier also specifies that these rates include the cost of the license and that of the servers dedicated to content recognition. These are services provided to customers so that they can ferret out illegal content on the Internet (using *web crawling*). It is expected that they will be adjusted with the adaptation of Article 17, which

also involves implementing licensing agreements, with a monetisation function, thus potentially enabling a price decrease, the company has stated.

<b>Reference collection size</b> (as described above)	<b>Different pricing based on daily query throughput</b>				
	< 100,000 images (< 500 video hours)	< 250,000 images (< 1,250 video h)	< 1 mio. images (5,000 video h)	< 2.5 mio. images (< 12,500 video h)	< 10 million images (< 50,000 video h)
up to 1 million images (5,000 hours of video)	990 \$	2,390 \$	5,990 \$	8,990 \$	10,990 \$
1 – 2.5 million images (< 12,500 hours of video)	2,390 \$	4,990 \$	8,990 \$	12,990 \$	14,990 \$
2.5 - 10 million images (< 50,000 hours of video)	5,990 \$	8,990 \$	10,990 \$	14,990 \$	17,990 \$
10 - 25 million images (< 125,000 hours of video)	8,990 \$	12,990 \$	14,990 \$	20,990 \$	25,990 \$
25 - 100 million images (< 500,000 hours of video)	10,990 \$	14,990 \$	17,990 \$	25,990 \$	29,990 \$

Figure 13

Audible Magic also operates on a licensing model.

<b>Audible Magic – Catalog price (per month)</b>		
<b>Input stream for analysis (in umber of videos)</b>	<b>Music recognition</b>	<b>Recognition of video soundtracks</b>
Up to 10,000	\$700	\$420
Up to 100 000	\$3250	\$1625
Up to 1 million	\$11000	\$6750
Up to 10 millions	\$28000	\$17000

Figure 14

Another economic model is that illustrated by the American company PEX. The use of its technology and its reference base is not dependent on the payment of user fees by the platform, but on the repayment of a fraction of the monetisation generated by the protected content. For example, according to the information provided by PEX to the mission for illustrative purposes (the rate ultimately being determined by *negotiation on a case-by-case basis*), if the advertising revenue distribution key is 45% for the platform and 55% for the beneficiary, the use of the PEX recognition solution could be priced at 5% of this revenue, with 55% remaining for the beneficiary and 40% for the platform.

2.2. – Rightholders: the wide range of expectations when it comes to recognition tools echoes the diversity of their situations with respect to sharing platforms.

Depending on the creative sector involved, sharing practices for user-protected content are perceived either (for music) as important channels for distributing content, with rightholders aiming to improve economic performance, or (for the audio-visual sector) as an illicit means of distribution, which must above all be clarified and regulated to protect exploitation methods that ensure better exploitation. As to sectors (in particular still images and written content) where platforms have not deployed tools for recognising and deriving profit from content, rightholders see them as a partner in the making, with strong demands. The expectations of rightholders therefore stand out for their significant heterogeneity, which is due as much to the diversity of their economic model as to that of their current relationship with the platforms.

2.2.1. - Film and audio-visual producers and distributors favour the blocking function to preserve the economic value of their rights.

*2.2.1.1. - The blocking function has priority, as platforms appear to be a risk factor for other, more profitable modes of operation.*

Audiovisual rightholders, first and foremost film producers, have made strong appeals to platforms to block the sharing of their content by users. The presence of this content on sharing platforms is perceived as a threat to other means of commercial operation, premised on the exercise of exclusive rights following the logic of media chronology. It is only in a much less central manner that these rightholders can use the monetisation function, mainly for trailers, and sometimes more rarely for excerpts or low-value works.

In this regard, as part of the implementation of Article 17 of the Directive on copyright in the Digital Single Market, the Motion Picture Association (MPA) insists on guaranteeing the freedom of its members not to enter into licensing agreements with platforms, and to choose to block content sharing.

With regard to this priority imperative, cooperation with sharing platforms and social media that have implemented recognition tools seems to be viewed positively: it emerges from the interviews run by the mission that, very generally, the performance of recognition tools in blocking the sharing of protected content is viewed by this sector as satisfactory.

In this sector, rightholders do not object to excerpts of their content being shared on platforms. While platforms offer recognition and blocking parameters that can be set based on recognition of a 30-second excerpt, and now 15 seconds, rightholders in the audio-visual sector (excluding television channels) seem to have opted for more permissive management rules, by accepting the sharing of longer-lasting content. For example, the one-stop-shop for fingerprinting operated by the ALPA (Association for the fight against audio-visual piracy) has opted for a period of several minutes. It

appears that at least some of the American studios have adopted similar practices. The duration of the content beyond which blocking is requested is generally sufficient to allow the presence on the platforms of brief excerpts with what appears to users as a form of implicit consent of the rightful owner.

In any case, the rightholders in this sector wish to ensure that recognition tools remain highly effective, seeing the ever-greater inventiveness of certain users in transforming content in such a way as to thwart the effectiveness of recognition tools. The satisfaction voiced therefore does not preclude high expectations on performance.

In the same vein, the mission has heard requests for improvements to the way claims are managed, in cases where it is not automated, as it is perceived as time-consuming and thus costly.

### *2.2.1.2.- The widespread use of recognition tools in the field of cinema still has room for progress.*

The effectiveness of the tools, as demonstrated in particular by the experience of rightholders at the international level, has led the French public authorities, and in particular the National Centre for Cinema and the Moving Image (CNC), to promote recognition tools and invite rightholders to produce fingerprints so that works can be protected.

Within the framework of the Association for the Fight against Audiovisual Piracy (ALPA), a “one-stop shop” has been set up, after an agreement concluded with Google on 19 September 2017 under the aegis of the CNC, intended to facilitate for the filing of fingerprints for rightholders in each platform reference base.

This agreement, which makes it possible to centralise the generation of fingerprints and manage conflicts with users or other rightholders, in accordance with rightholder preferences, is innovative and an attractive service offer for ALPA members. In particular, it takes into account the reluctance of certain rightholders to deliver their content to the platforms so that they make the fingerprints themselves. The system implemented by ALPA has therefore provided for the use of a service provider that can be tasked with making fingerprints which it later delivers to the platforms, without the latter therefore having the content. However, protection by the latest generation of fingerprints remains reserved for rightholders who deliver their content<sup>29</sup>, as YouTube wishes to be the sole party implementing the latest generation of fingerprints. What’s more, YouTube does not guarantee back-compatibility of fingerprints when a new version is introduced.

The approach taken by ALPA, which aims to promote content recognition tools, is primarily aimed at its members or those who agree to join it and is based on a voluntary act by the rightholder. The information produced by ALPA in any case shows that even film producers who might have an interest

---

<sup>29</sup> Given the constant improvement in technologies, YouTube regularly rolls out new versions of digital fingerprints (approximately every six months). When it has the content, it ensures the back-compatibility of fingerprints by creating the latest generation of fingerprints for all this content.

in protecting their content are not always aware of the recognition tools available on the platforms or do not implement them.

Thus, it may happen that works are available on the platforms without this resulting from a deliberate choice by the rightholders: because no fingerprint has ever been made, because the fingerprint made has not been updated, or because they believe they should rely on a distributor or a broadcaster.

Furthermore, a major French producer of animated films, who did not wish to be identified in the report, spoke to the mission about the issues he had encountered for some time with YouTube to ensure due protection for his works: whereas the platform encouraged him to choose content monetisation rather than blocking, and whereas that monetisation enables the platform to better promote its search engine, the producer stood by his choice of content blocking in principle, with only very partial monetisation, but had to go through the intermediary of the broadcaster, which has more clout regarding YouTube, to protect his content. The same producer also stated that he had experienced difficulties in laying claim to certain content on which third-parties had made illegal fingerprints: it proved exceedingly difficult to have these removed and replaced by his own authentic fingerprints. In addition to fingerprint and interface effectiveness, the platform must work on the quality of its relationships if it is to successfully overcome the problems that arise, even in the most complex cases.

*2.2.1.3. - In some cases, actors are still uncertain as to who should be responsible for registering and managing fingerprints: producers or distributors.*

One of the possible reasons for which protected films can be found on a platform, aside from (rare) cases of rightholder choice or escheat, is a lack of coordination between the various actors along the production and distribution chain of cinematographic works.

Some producers continue to feel that it is up to the distributor(s) to generate a fingerprint, so as to ensure the protection of the content which they purchase. They may be of the opinion that the protection of rights is the responsibility of distributors, who know their operating territory and who can better choose what use to allow, based on local characteristics.

In other instances, on platforms that offer this option, producers and distributors end up generating a fingerprint for the same work, which can lead to conflicts in management rules.

The CNC deems that the generation of fingerprints by producers, as per the model used in the one-stop shop set up by ALPA, offers the advantage of being both efficient and stable, as the rights of producers are by nature more lasting over time and less restricted at the territorial level. It has thus initiated long-term information and awareness-building aimed at producers, bringing to light the advantages of the one-stop shop operated by ALPA. In this context, on 11 July 2019, it took the initiative to bring together, around the one-stop shop, the professional organisations of producers,

distributors, collective management organisations, YouTube and ALPA. It is important that such action be continued.

#### *2.2.1.4. - Content blocking on platforms as part of an integrated intellectual property rights protection policy.*

From the producers' standpoint, the presence of unauthorised content on platforms is only one aspect of the fight against the illegal distribution of content, another part of which concerns so-called massively illegal operators (streaming and direct downloading).

Producers are thus implementing an integrated approach to the protection of their intellectual property, most often through specialised service providers. They thus offer both verification on the platforms, to ensure the effectiveness of recognition tools through targeted manual searches, and action to fight streaming and direct download sites.

#### *2.2.1.5. – Audiovisual authors' collective management organisations have signed agreements with certain sharing platforms.*

In France, the authors' societies in the audio-visual field (SACD and SCAM, to which must be added SACEM) already have extensive experience of agreements with sharing platforms. Long-standing signatories of collective agreements through which they receive income from broadcasting by television channels, they began signing agreements from as early as 2008 (Dailymotion) and 2010 (YouTube), a decision challenged at the time by certain organisations of audio-visual producers.

This experience, which enables these companies to receive, as do the SACEM for music operations and the ADAGP for visual arts, a percentage of the platform's advertising revenue as determined by contract (rather than a share of the revenue from monetising data videos) remains limited to certain platforms (there is no agreement with Facebook). It appears to be particularly well-developed in France as opposed to other European countries, presumably reflecting the tradition of collective bargaining, also illustrated by agreements between audio-visual authors' societies and television channels.

While these agreements enable authors' companies to receive remuneration for the use of their members' works on the platforms, they have also given them the chance to expand their repertoire of authors with content developed specifically for the platforms. In particular, videographers who own channels, particularly YouTube, have joined SCAM and SACD to benefit from the copyright collected by these companies pursuant to the agreements concluded with the platform.

Given the massive presence of their content on the platforms, while other audio-visual content is subject to heavy restrictions due to their producers' preference for blocking policies and other modes of commercial use, it is these authors of native content on the platforms who appear to receive most of the distributed rights.

The audio-visual authors represented by the SACD and SCAM generally do not claim to have control over content recognition tools, the management of which is the responsibility of producers<sup>30</sup>. As far as videographers are concerned, it is in their capacity as producers (as they are often authors and producers) that they are interested in the issue of content recognition (see below).

2.2.2. - The main television channels have come to make intensive use of content recognition tools.

2.2.2.1. - *Television channels prefer to have their content blocked, including short excerpts.*

Like cinema rightholders, television channels generally use recognition tools to block the distribution of their content on platforms, so as to preserve the exclusivity of their own broadcasting channels (websites and catch-up television offers). Any accounts which they might hold, directly or through the producers of their shows, on social media therefore tend to be used primarily for promotional purposes. This concern for keeping control over their broadcasting channels was behind the decisions made, for instance, in recent times by France Télévisions, whereas in the past, priority had been given to maintaining a wider range of content on platforms.

Given how important it is for them to ensure that content is actually blocked on platforms, broadcasters are keen to see a continuous improvement approach adopted with respect to protection tools. TF1 informed the mission that it had asked to be provided with data regularly, so as to verify the effectiveness of recognition tools, either directly or through a public authority. It asks that any incident in the functioning of the recognition tools, for example in the event of a breakdown, give rise to prompt measures to inform rightholders, along with information on the corrective measures taken<sup>31</sup>.

Protection for broadcasters' programmes also poses a special difficulty when identical video content which they broadcast and on which they could therefore generate fingerprints is in fact already protected. This is the case, for example, with news videos produced by a shared "pool image", then broadcast by multiple channels, or when a given channel replays excerpts from another channel's

---

<sup>30</sup> The SACD has established a template clause incorporated into the standard contracts which it offers between author and producer, giving the latter the obligation to protect the work, in particular using the fingerprinting technique.

<sup>31</sup> Excerpt of TF1 contribution : "Automated content recognition algorithms could be subject to biases, deliberate or not aiming at secretly undermining their performance in order to facilitate, even temporarily, (for example via code injection which would be withdrawn after a certain period) the introduction of counterfeit content despite existing fingerprints made by the rightholders. This is why it seems essential that at least a public authority can have access to algorithms used by automated content recognition tools, so as to verify the absence of such biases. Otherwise, there is no guarantee that such algorithmic biases do not exist at the expense of rightholders. Any open, public, transparent and documented solution must be preferred, in full accordance with the objective of algorithmic transparency, like the SIFT algorithm used by the Icelandic company Videntifier, and apparently implemented by Facebook; but we still then need to know the terms and conditions of deployment of such a solution. Algorithmic transparency, in the field of automated recognition of content in order to preserve rightholders and copyright, appears as an essential prerequisite for the principles of trust, transparency and collaboration, which govern the spirit of the Directive. In the same spirit of continuous transparency, TF1 also wishes that any incident during the operations of the recognition tools, for example in the event of a breakdown, lead to a rapid information for rightholders, with details such as the source of the failure and the corrective measures taken."



programmes (in a “channel-hopping” type programme). This means that broadcasters, at the risk of facing more and more conflicts over ownership of rights, must refrain from generating footprints for those types of content that can be reproduced by others or from using the “white list” technique for certain channels.

#### *2.2.2.2. - Some broadcasters, however, complain that fingerprinting tools are ill-adapted.*

Some specialist channels, whose audience is smaller than that of general channels, shared with the mission their difficulties with the recognition tools offered by platforms.

The first difficulty emphasised can be summarised as access to fingerprint registration for such channels. RMC Découverte and RMC Story (both of which are Altice Group channels) for instance told the mission of their difficulties in accessing Content ID. They called attention to “strikes” which they received due to fingerprints previously placed on the content they broadcast (possibly denoting prior protection by other rightholders, audio-visual producers or distributors, or sports rightholders). The platform also reportedly pointed out the relatively low volume of original content on these channels.

These channels regret that they are not offered an alternative protection option (e.g. based on a combination of recognition of their channel’s logo and a fingerprint made on the soundtrack). They also point out the complexity and limitations of the notification tools which they become required to use if their program is taken up by users (number of notifications limited to 10 per day).

Lastly, they emphasise that, once they were able to gain access to fingerprint registration, they came upon another issue, as they could not set the length of the protection sought to match the duration of the rights they held, and were thus required to accept complex management procedures over the longer term.

#### *2.2.2.3. Broadcasters are keen on ensuring that tools are deployed to protect live broadcast content on platforms.*

Dedicated to promoting the direct content in which they make significant investments, particularly when it comes to sporting rights, broadcasters are watching closely, in this area as well, to see whether platforms will deploy effective recognition tools.

Effective protection of rights requires that fingerprints be generated as each live stream is broadcast, so that platforms can spot the potential upload of that stream and block it. It also requires that the channels and platforms set up dedicated mechanisms when broadcasting important events: manual monitoring of platforms carried out by the channels, while the platforms set up teams capable of blocking any accounts that broadcast protected content despite the use of recognition tools, immediately upon receiving notice of their activity.

2.2.3. - The vast majority of music rightholders have licensing and monetisation aims.

*2.2.3.1. - Phonogram producers have made sharing platforms their major partners.*

Phonogram producers use the blocking feature primarily to protect recordings before they are released and in certain specific cases of exclusivity. For them, the aim is to prevent new products from being leaked before their official release date, within their work to manage a highly supervised production line, where the generation of fingerprints for each of the platforms is an essential step.

Apart from this distinct situation, fingerprint recognition tools are mainly used to monetise content distributed on platforms with which producers have signed licensing agreements providing that any income generated will be shared.

Producers have spearheaded the demand to improve the contractual terms offered by platforms, an effort that resulted in the adoption of Article 17 of the European Directive (theme of the transfer of value or “*value gap*”). Their objective is both to establish a more balanced contractual relationship than that which prevailed so long as the platforms claimed their status as hosting provider and to be allocated a more significant share of the revenues generated on the platforms when content from their catalogues is shared.

*2.2.3.2. - The collective management organisations representing songwriters and music publishers are also geared toward licensing.*

Like its European counterparts, SACEM has, over the last ten years, developed a tried-and-true contractual relationship with the largest sharing platforms. In 2010, it signed its first contract with YouTube, renewed several times since, the latest version covering the catalogues of SACEM members and the Anglo-American catalogues of Universal Music Publishing, of which YouTube is thus entitled to make commercial use in 168 countries. Its British counterpart, meanwhile, has been under contract since 2007. As to the German counterpart, GEMA, it signed an agreement in 2016, bringing to an end a long-running dispute that had led, at one point, to widespread blockages of music videos on YouTube in Germany. SACEM has signed agreements with other services as well: in addition to the agreements that have existed with Dailymotion, these include Facebook since 2018, as well as SoundCloud. Lastly, to use another European example, the ICE alliance, which includes the British (PRS), German (GEMA) and Swedish (STIM) collective management organisations, has signed agreements with Facebook and Soundcloud.

The implementation of these agreements for copyright holders, however, raises specific difficulties in the use of fingerprinting technology. Namely, the recognition tools deployed by the platforms, based on fingerprints made from the recordings and therefore the producers’ related rights, give only an indirect and partial view of the use of music copyright, though they do make it possible to distribute monetisation revenues to producers. Complex reconciliation work is needed in order to assign rights

to authors. Furthermore, the fingerprints made from the recordings cannot be used to ascribe rights to authors for in-concert performances for which no fingerprint has been made, or for covers of songs, for example by users (which are considered acts of commercial use, within the meaning of copyright but obviously not within the meaning of the producer and performer rights), whereas concert recordings and covers by other performers can account for a considerable proportion of the music found on platforms and covered by copyright. While YouTube has rolled out a tool specific to this area, known as Melody ID, the way in which it is implemented and its results are still subject to considerable uncertainties, and the other platforms do not appear to be equipped with comparable tools.

Wishing to both resolve this difficulty and to establish a more balanced contractual relationship with the platforms than that which prevailed so long as the platforms invoked their status as hosting providers, the collective management organisations serving songwriters and music publishers, represented by the GESAC (European Grouping of Societies of Authors and Composers), were very active in their support for the proposals on which Article 17 was premised. They did a great deal to promote understanding about the *value gap* issue, pointing out that the remuneration received from sharing platforms was significantly lower than that received from other online services giving access to their works.

#### 2.2.4. - Rightholders in other sectors do not have recognition tools deployed on the platforms.

Even though the works in their catalogues are widely shared on digital platforms, holders of copyright and related rights in the visual arts, writing and video game sectors do not have access to recognition tools, either because the sharing platforms refused to take their requests into consideration, or because they did not submit any requests.

##### *2.2.4.1. - Rightholders in the visual arts have been unable to secure the platforms' consent to implement appropriate recognition tools, but are ready to sign licensing agreements with the platforms.*

Upon learning that works from their catalogues are found on certain platforms, visual arts rightholders, in particular when still images are involved, can do little more than file a take-down request, which is ineffective insofar as copies resurface. This is because the platforms have not set up automated recognition tools, thus putting visual arts rightholders in a much less favourable position than those in the audio-visual or music sectors.

This situation is the result of the “host provider’s status” which sharing platforms have invoked up to this point,<sup>32</sup> and which certain rightholders in the still images sector unsuccessfully challenged, as had rightholders in other sectors before them.

Although they have often focused their legal actions on image referencing and display services (such as Google image search)<sup>33</sup>, many rightholders in the field of still images believe that sharing platforms engage in unauthorised acts of presentation to the public of works belonging to their members. Such was the case when ADAGP came into conflict with Flickr (2007-2009): the court ruled that it had to provide the platform with the catalogue of the 25,000 works on which it claimed rights. The rightholders in this sector have only rarely been able to sign agreements (as is the case with ADAGP) or, in certain cases, secure marginal improvements in the functionalities of certain platforms<sup>34</sup>.

Holders of still image rights are aware of the difficulties inherent in determining the presence of their works on platforms. When, in the case of ADAGP, an agreement was successfully signed regarding the presence of its catalogues on YouTube, ADAGP then had to define a method to substantiate the actual presence of the works of its catalogues on the platform.

Because no recognition tool had been instituted by the platforms, ADAGP had to develop its own tool, working with CISAC; still in the making, it will enable the organisation to trace the presence of works from its catalogue on the Internet as a whole, and in particular on the platforms. The resulting tool, called AIR (*Automated Image Recognition*), will not be able to inventory the entirety of the French catalogues online like that of other participating sister collective management organisations, given the very large volume of catalogues involved, but may help identify how they are used.

Furthermore, the still images rightholders whom the mission met emphasised the importance of ensuring that platforms stop removing the metadata attached to image files, as is currently standard practice, firstly as a matter of compliance with moral rights but also to effectively monitor uses.

Lastly, and more specifically with regard to 3D artwork modelling files, while some platforms do offer them (Cults3D.com, Myminifactory.com, Primante3D.com, Thingiverse.com), the related audience appears small and the question of possible protection of uses due to sharing does not seem to be of relevance at present, precisely because sharing of this type of file remains marginal.

---

<sup>32</sup> Including when agreements were, by way of exception, signed by the sharing platforms with rightholders, for instance, YouTube and Dailymotion with ADAGP.

<sup>33</sup> See in particular the legal action initiated in vain by SAIF (Société des auteurs de l’image fixe) against Google which gave rise to a ruling by the Paris Court of Appeal of 26 January 2011 (copied here: [http://data.over-blog-kiwi.com/1/13/34/21/20140707/ob\\_0239d9\\_jugement-ca-paris-26-janvier-2011-goog.pdf](http://data.over-blog-kiwi.com/1/13/34/21/20140707/ob_0239d9_jugement-ca-paris-26-janvier-2011-goog.pdf)). Similarly, in 2016, Getty Images filed a lawsuit against Google over the Google Image service, but went on to withdraw it in 2018, under a licensing agreement that also reportedly included changes to certain linking practices.

<sup>34</sup> To read the agreement signed by Getty Images with Google for the Google Images service, see: <https://www.siliconrepublic.com/companies/google-view-image-getty-deal>

#### *2.2.4.2. - Rightholders of written content are not provided with appropriate recognition tools on sharing platforms.*

For holders of book rights, content-sharing platforms are primarily connected with the fight against the distribution of illegal copies. Moreover, they are not necessarily the main issue today; their concerns relate more to piracy and file-hosting sites (“cyberlockers”).

The focuses reported to the mission do, however, include unauthorised audio book sharing practices. Audio books, which have the same technical characteristics as a piece of music, can be protected by an audio fingerprint. Even if some publishers have done so (for instance, Hachette Livre), it appears that not all audio book publishers have been interested in adopting this tool. Furthermore, audio book fingerprinting requires publishers to engage in automated blocking, albeit sometimes unwanted, causing such publishers as Hachette Livre to include certain so-called “booktubers” in its white list.

Another current trend highlighted by publishers is the uploading of comic strips and even more of manga, recorded as an anonymous hand turns the pages. Publishers are not equipped to deal with this trend, and can do nothing but notify the platforms of the content's presence and wait for it to be taken down. The technical feasibility of creating a fingerprint has not been tested.

As to press publications, no platform has yet set up tools to recognise the text. Press publishers focused their attention on sharing value through search engines and content aggregation services, such as Google News, a subject distinct from sharing platforms.

Meanwhile, publishers of scientific, technical and medical press have made content take-down requests into regular practice. The company ReIX succeeded in obtaining site-blocking court orders in France (Sci Hub and The Library Genesis) in 2019<sup>35</sup> and won damages from the US courts in 2017 for copyright infringement<sup>36</sup> by similar platforms.

With regard to the ResearchGate platform, scientific publishers have called for recognition tools to be set up to block and remove unauthorised content.

This platform, set up for the research world and specialised in technical and medical scientific publications, became the target of legal proceedings in Germany by publishers in the field. They have formed a “Coalition for Responsible Sharing” and reports having secured the removal of 1.2 million items from the platform, or a purported 92% of the content belonging to coalition members. The coalition has so far been unsuccessful in convincing the platform to implement an automated blocking and removal tool. Even if the platform were to agree to the request, it would in principle hold on to the option of receiving the findings of any research submitted, so long as it does not include the intellectual property held by publishers.

---

<sup>35</sup> <https://www.legalis.net/jurisprudences/tgi-de-paris-3eme-ch-4eme-section-jugement-en-la-forme-des-referes-le-7-mars-2019/>

<sup>36</sup> <https://www.actualitte.com/article/monde-edition/le-site-sci-hub-condamne-a-payer-15-millions-pour-atteinte-au-droit-d-auteur/83499>

Generally speaking, book and press rightholders expect platforms to better take into account their rights, all the while acknowledging the limitations of recognition tools when it comes to some of their rights.

*2.2.4.3. - Rightholders in the video game industry, in their relations with sharing platforms, appear at this stage to favour the presence of their content for visibility purposes.*

Sharing platforms, which are not considered vehicles distributing illegal copies of video game software and incidentally do not enable play of the same, are perceived by rights holders in this sector as very important promotional windows: gaming activity helps showcase the products developed, and is a speciality of such platforms as Twitch.

Nintendo, however, made a name for itself by creating the Nintendo Creator's Program (NCP) in 2015. By registering fingerprints through the programme, Nintendo implicitly laid claim to the monetisation revenue stemming from the dissemination of the images and sounds of the brand's video games while the corresponding revenue would be shared with users agreeing to save their games and upload the related content to the platform. Players not subscribing to the NCP would be deemed to leave to Nintendo the revenue from their uploads and on which the brand's video games appeared. The programme was discontinued in 2018. Now, Nintendo allows, more broadly speaking, the use of game footage in the videographers' works, subject to certain conditions<sup>37</sup>, primarily drafted to ensure due respect for its intellectual property rights, though this has not prevented some such players from publishing footage of their Nintendo play online and deriving revenue from it.

Also of note are cases in which videos have been blocked due to the presence of content belonging to video game publishers, in particular cinematic sequences that sometimes appear during game sessions. These cases are generally reported by rightholders other than the owners or publishers of video games, for example a television channel that broadcasts live a game, which it protects with a fingerprint. Those who played the recorded game can then find themselves blocked from sharing their own footage, the recognition tool having identified the content from the fingerprint made using the TV programme.

*2.2.4.4. - Publishers managing rights to the “graphic commercial use” of music (scores and song lyrics) do not have the benefit of recognition tools.*

Those publishers who hold music rights for “graphic commercial use” (scores and lyrics of songs the rights of which, as far as French publishers are concerned, have not been entrusted to SACEM and instead are individually managed by publishers) call attention to the magnitude of unauthorised

---

<sup>37</sup> [https://www.nintendo.co.jp/networkservice\\_guideline/fr/index.html](https://www.nintendo.co.jp/networkservice_guideline/fr/index.html)

sharing of works in their repertoire. In particular, they point up practices such as subtitling music videos or even sharing karaoke.

In the absence of recognition tools, rightholders in this sector are forced to request to take the content down, which are cumbersome and not always understood by the platforms, not very sensitive to a lack of knowledge of rights from which their holders in other countries do not always attempt to derive value.

The *Chambre Syndicale de l'édition musicales* (CSDEM) has developed a reference base, called BOEM, for song lyrics, available on the site [paroles-csdem.com](http://paroles-csdem.com). Its content is subject to licensing, the response found to monetise its value in a context where no recognition tool has been set up for text in the field of music.

2.2.5. - The expectations of rightholders with respect to content recognition tools are thus varied, reflecting the differences in practice, depending on the sectors and the size of the actors.

The diverging expectations of music and audiovisual rightholders can be explained first of all by the predominant preference for monetisation by the former, and for blocking by the latter, a difference itself ascribable to the economics of the respective sectors. In music, platforms are perceived as a distribution channel that competes directly with other channels, and whose rightholders expect comparable remuneration. In the field of cinema and audiovisual media, they are seen first of all as a channel for distributing unauthorised copies, hence the massive preference for blocking, secondly as a promotional showcase and lastly, to a lesser extent, as a monetisation space offering only limited income reserved for certain content.

Within these two sectors, it is the largest actors, fully integrated into the logic of the fingerprinting system, that are most likely to see the management tools offered to them by the platforms in a positive light. They are keen on seeing these tools effectively used, and thus, in the event of dispute with a user contesting a block, on having control over the decision as a last resort. Other players, less influential, either do not have access to the same tools or are still looking for other protection solutions. The implementation of recognition tools and the release of functionalities in step with rights management needs were determined by the balance of power in place, and by the interests of the most powerful international rightholders, their French counterparts sometimes adopting the same approach, but later (e.g., cinema). In the relationship between rightholders and sharing platforms, France remains unique for the place which collective management organisations representing authors have been able to make for themselves, having had to define the means by which any use of their repertoire would be identified without being able to rely on the fingerprinting system alone, defined on the basis of the rights held by producers.

The main criticisms voiced with regard to recognition tools by users-rightholders concern, in addition to the resources required to effectively manage them: the technological gap that has developed between the most advanced platforms and certain others; and the issue of protected works and

subject matter not taken into account (visual arts) or taken into account on the basis of fingerprints made by other rightholders (SACEM).

Differences in treatment as expressed in access to recognition tools and the definition of the functionalities offered to rightholders are also frequently criticised, as the criteria or conditions for access are often considered intentionally obscure. At the current time, fingerprint registration plays out *de facto* as presumptive ownership of rights; only for some rightholders does it result in access to shared content take-down features.

Rightholders pay particularly close attention to how disputes from users are addressed, with the fear that in the future they will be required either to provide too much justification for their requests or make decisions too quickly. They expect the platform, regardless of the tool used, to assume their good faith, pointing out that blocking and take-down contestations are often unjustified and sometimes even highly imaginative.

## 2.3. – Users perception: widely-varying experiences on the ground, acceptance of copyright rules in principle, and implications with regard to the availability of content.

An *ad hoc* quantitative study conducted by Hadopi appears to indicate that in France (2.3.1), users, despite the diversity in uses and a wide range of levels of involvement (2.3.2), seem to understand and accept the impact of copyright on the availability of content on platforms (2.3.3).

### 2.3.1. - Presentation of the quantitative study methodology.

Hadopi's *ad hoc* quantitative study was aimed at studying in detail the behaviour of Internet users on content sharing platforms and the usage issues encountered. This study was carried out on a representative sample of French Internet users ages 15 or above, interviewed online. It was carried out by the OpinionWay institute.

It was based on a two-step methodology:

- the initial scoping phase, on a sample of 3,040 Internet users ages 15 and over, representative of the French population (quota method), took place from 19 August to 4 September 2019. This phase had two main aims: first of all, to measure French Internet users' level of understanding when it comes to copyright rules and the consequences thereof on the availability of content on platforms, and secondly, to measure the penetration rate and profile of Internet users who have had to content with measures to block content they posted online;
- a second phase, limited to a sample of 1,445 Internet users who had shared audiovisual and video content, including a base of 285 Internet users who had actually been subject to blocking measures, was run from last 21 October to 15 November 2019.

This phase offered the opportunity to study in depth the blocking of content put online by Internet users: type of content blocked; grounds for blocking and how the receiving Internet



users understand it; outcome of the blocking process, including, possibly, the return of the content online.

## 2.3.2. - Massive use of the social media, with varying degrees of user involvement.

### 2.3.2.1. - Massive use of the social media.

The study commissioned by Hadopi first makes it possible to draw up an inventory of the uses of social media and content sharing platforms, in general and for content sharing purposes.

Six content sharing platforms were considered in the quantitative study: Facebook, YouTube, Instagram, Twitter, Dailymotion and Reddit.

The study indicates that 80% of Internet users have at least one account on the social media and content sharing platforms (and 49% have more than account). The most widely used networks are Facebook, on which 71% of Internet users have an account, followed by YouTube (38% of Internet users registered).

**Registration rate on social media – base: internet users (3029 ind.)**

<b>Account-holders...</b>	<b>Among Internet users</b>
<b>At least one account</b>	<b>80%</b>
<b>One Account</b>	<b>31%</b>
<b>Multiple Accounts</b>	<b>49%</b>
Facebook	71%
YouTube	38%
Instagram	34%
Twitter	23%
Dailymotion	6%
Reddit	2%

Figure 15

Source: OpinionWay study for Hadopi, 2019

The intensity of use of these networks varies greatly depending on the type of platform; two groups can be distinguished: platforms whose use has become part of the everyday (Facebook, Instagram), and platforms that stir less involvement from their users.

### Intensity of use of social media – base: Internet users with an account on the platform studied

Figure 16

Daily intensity of use	Social media	Daily or almost daily use	
		Among users	Among Internet users
High	Facebook	69%	50%
	Instagram	63%	23%
Average	Twitter	45%	11%
	YouTube	37%	24%
Low	Reddit	36%	1%
	Dailymotion	16%	2%

Source: OpinionWay study for Hadopi, 2019

#### 2.3.2.2. – Diversity in uses.

Users must hold an account in order to upload content on the social media. On YouTube or Dailymotion, however, no prior registration is necessary for viewing and “sharing”. It is indeed possible to “share” (or relay) YouTube videos on other social networks such as Twitter or LinkedIn, without having a YouTube account.

Furthermore, the use of social media such as Facebook or Twitter, while theoretically possible without an account, proves of little interest to users: it can thus reasonably be deemed that almost all users of these platforms have an account.

To wit, 73% of the Internet users with at least one account did share content on one of these platforms, i.e. more than half of Internet users (58%), and 33% of audio or video content (target that is the subject of the 2<sup>nd</sup> phase of the quantitative study).

YouTube usage, reported by 65% of Internet users surveyed (with or without an account), can be divided into three levels, according to the Internet user’s degree of involvement in the practice (such users will generically be referred to as YouTube users):

- the use of YouTube solely as a medium for viewing content. These platform users access content without registering on the site, and do not post any content to it. This type of use is found in 27% of YouTube users, i.e. 18% of Internet users;
- Account holders. YouTube users can post videos via their account, which will be visible to other users. This is the case with 59% of the platform’s users, i.e. 38% of Internet users;
- YouTube channel ownership. This is the most advanced stage of YouTube usage, and applies to 33% of YouTube account holders, or about 13% of Internet users. This last category includes in particular professional and semi-professional videographers.

The vast majority of YouTube channels have a small audience: 69% of YouTube channel owners have fewer than 500 subscribers (about 8% of Internet users), and 17% have more than 1,000 views for a single video (just 2% of Internet users).

The use of social media for profit is a practice that is still limited in France.

6% of Internet users state that they derive income from the content they share on the social media. This is particularly the case for owners of Reddit accounts (52% say they earn income from them), followed by Dailymotion (29%), Twitter (12%), Instagram (9%), YouTube (9%), and Facebook (6%).

Out of the Internet users who earn income on the social media, 69% state that they have already had all or part of their income allocated to another person illicitly using their work, i.e. around 4% of Internet users. In 41% of cases it was an excerpt, 38% a parody, 31% a remix and 28% an entire work.

2.3.3. While Internet users have a good understanding of the implications of copyright rules as applicable to content sharing platforms, their knowledge is more relative when it comes to the rules on exceptions.

Based on their assessments of a series of assertions as “true” or “false,” two-thirds of Internet users appear to have mastered the principle of authorisation required to share content. These responses reflect a certain level of familiarity with and understanding of copyright principles.

#### Opinion of Internet users on posting content

<i>In bold and colour: correct answer</i>	TRUE	FALSE
Posting excerpts from music or films by another author does not require permission	31%	<b>69%</b>
Posting musical scores online does not require authorisation	32%	<b>68%</b>
Posting a live video of one's television as it shows the broadcast of a competition does not require authorisation	35%	<b>65%</b>

*In green: correct answer*

Figure 17

Source: OpinionWay study for Hadopi, 2019

More precisely, 87% of Internet users are aware that platforms can remove content and 75% know that they can also prevent cultural content from being posted.

### Opinion of internet users on platforms' scope for action

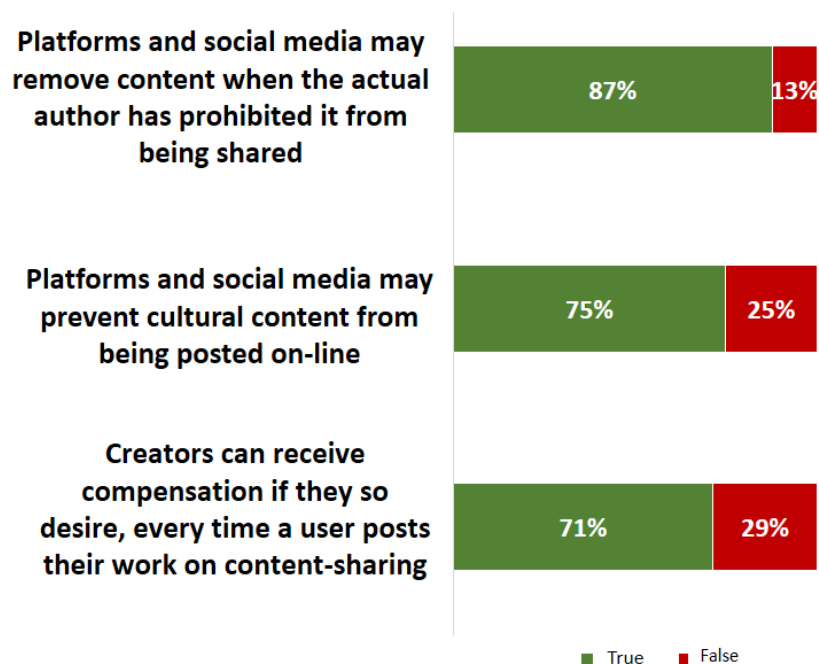


Figure 18

Source: OpinionWay study for Hadopi, 2019

French Internet users claim to have good knowledge of recognition tools: 71% are familiar with the concept of content blocking (77% of audio/video content providers); more specifically, 46% are aware that content can be blocked, and 43% that content can be identified.

However, French Internet users are not always familiar with exceptions to copyright. For instance, the concept of parody is fuzzy: 45% of Internet users deemed the assertion that no authorisation is needed to broadcast a parody to be false (the correct answer being “true”, there is no need for authorisation).

Moreover, the distinction between the concepts of representation, quotation and respect for the author’s rights-holding is not clear.

### Opinion of internet users on posting a parody and quoting

<i>In bold and colour: correct answer</i>	TRUE	FALSE
Posting a parody of music, a film or other cultural content does not require permission	<b>55%</b>	45%
Individuals may post content of which they are not the author if they clearly indicate who is the actual author of the content	67%	<b>33%</b>

*In green: correct answer*

Figure 19

Source: OpinionWay study for Hadopi, 2019

The rules implemented by the social media and platforms appear to be warranted, in the opinion of the vast majority of Internet users.

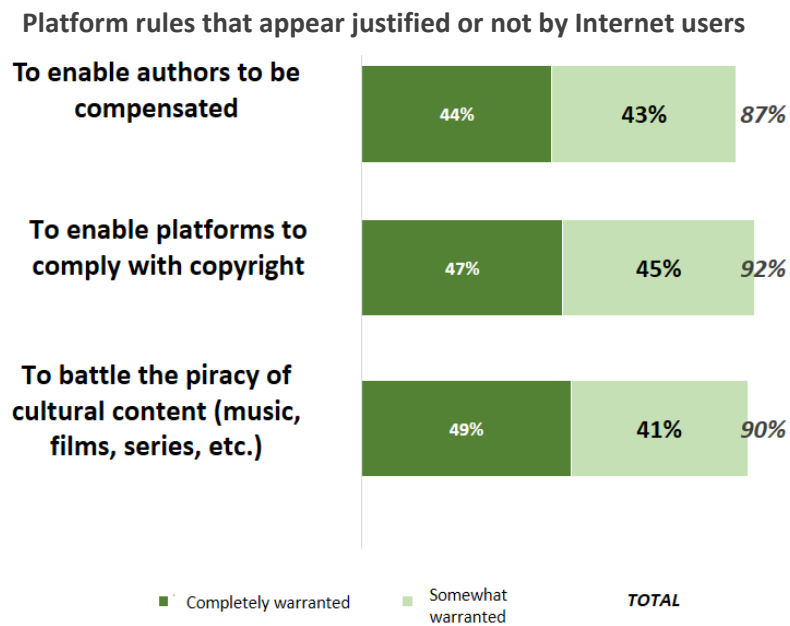


Figure 20

Source: OpinionWay study for Hadopi, 2019

However, once the questions move beyond the “rules implemented by platforms” to look into more concrete actions, Internet users are more ambivalent. On the one hand, they widely acknowledge the pre-eminence of authors prerogatives, authors having the right to oppose the distribution of their content (89% agree, 88% when it comes to blocking); however, on the other hand, this legitimate right enjoyed by authors to control their content is seen as censorship or an infringement of creation by almost half of Internet users (respectively 47% and 46% of Internet users).

**Opinion of Internet users on the ability to block or remove works by authors or platforms**

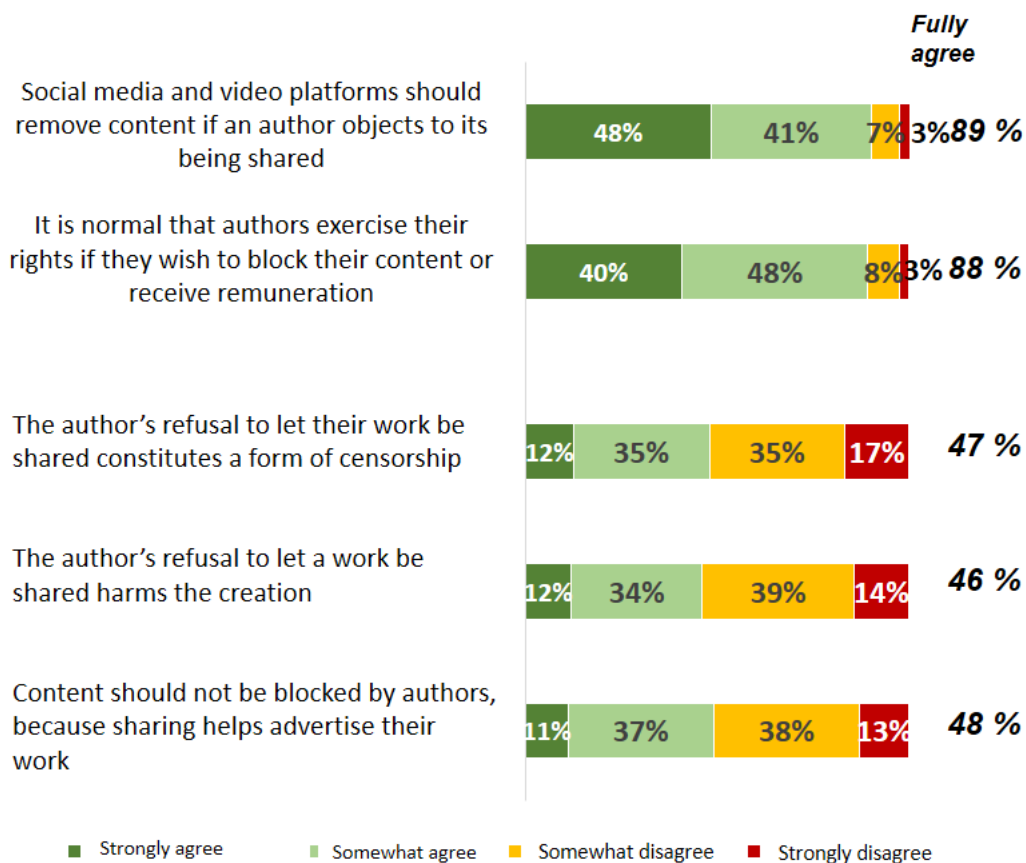


Figure 21

Source: OpinionWay study for Hadopi, 2019

2.3.4. - Many users have experienced blocking of their content on social media or platforms, and generally understand the reasons behind it.

2.3.4.1. - More than half of Internet users share content on platforms.

The study distinguishes between three types of content posted by users to set apart potential cases of copyright infringement:

- content exclusively personal to the user, which accounts for 42% of the shares of these internet users;
- content originating exclusively from persons other than the user (described as original works), which account for 24% of the acts of sharing;
- mixed content combining personal user content and content from third parties, which account for 19% of sharing actions.

More specifically, Internet users who share audio or video content (i.e. 33% of Internet users) equally share exclusively personal content (16% of Internet users) and exclusively original works (16%), with mixed content being shared to a lesser extent (11% of Internet users).

Content sharing – database: Internet users aged 15 and over

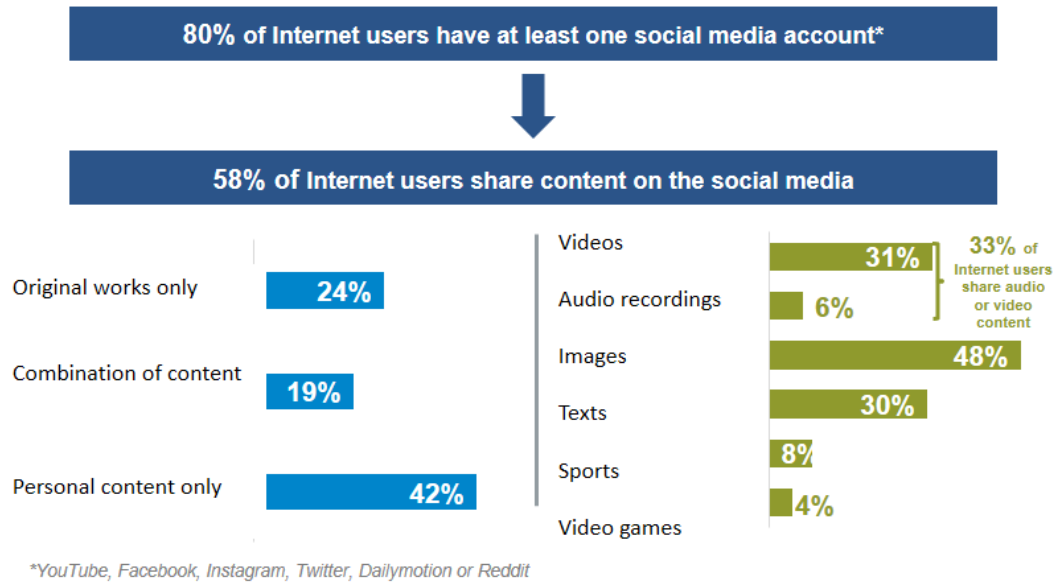


Figure 22

Source: OpinionWay study for Hadopi, 2019

Looking at the users by main platform:

- on YouTube, 58% of account holders have posted content before: 20% have posted content that is exclusively personal before, 15% content owned only by other people and 8% mixed content;
- on Facebook, 71% of account holders have posted content before: 46% of content that is exclusively personal, 26% of content that is solely owned by other people and 19% mixed content.

Considering the platforms' usage rate, Facebook, Instagram and YouTube are therefore the platforms most used by Internet users to share content:

Percentage of Internet users sharing content via social media

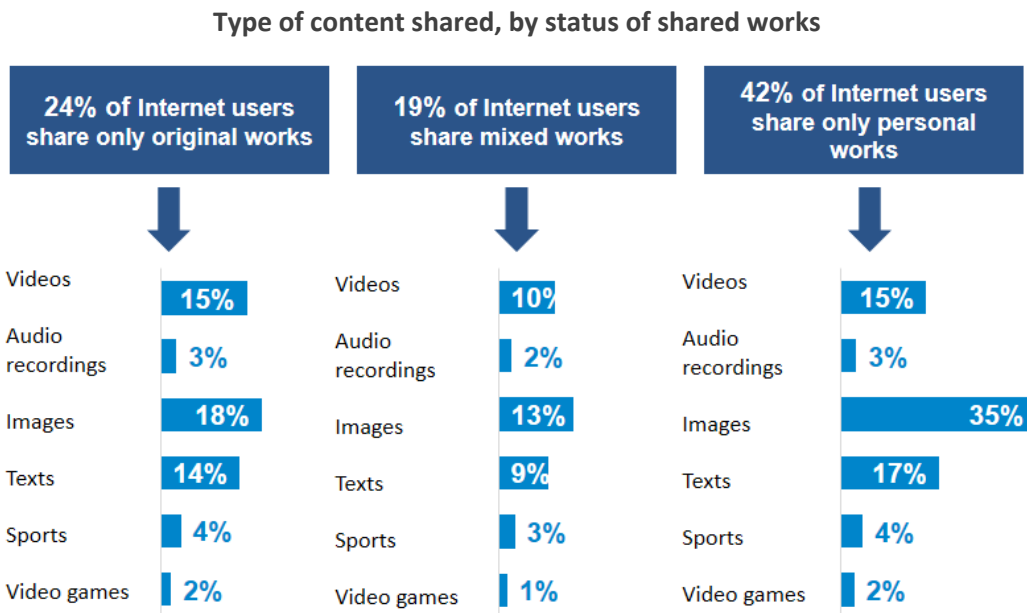
Percentage of internet users sharing content	Base: those with accounts on each network	Base: Internet users
Facebook	71%	50%
Instagram	71%	24%
YouTube	58%	22%
Twitter	63%	14%
Dailymotion	62%	4%
Reddit	79%	2%

Figure 23

Source: OpinionWay study for Hadopi, 2019

In more than half the cases of content sharing, the original works shared as incorporated into mixed publications were unaltered.

When the content shared is solely the property of other persons (without addition or modification), it consists mainly of images, videos or texts (respectively in 73%, 63% and 58% of sharing cases). Sports, audio recordings and video games are less shared (15%, 12% and 8% of cases). The same results can be observed when it comes to the publication of mixed content.



Database: Internet users ages 15 and above

Note to the reader: 24% of Internet users share solely original works, 15% share videos that are solely original works (videos therefore account for 63% of original works shared:  $15/24=63\%$ )

Figure 24

Source: OpinionWay study for Hadopi, 2019

### 2.3.4.2. - A minority of Internet users have been subject to blocking measures.

The majority of Internet users has had to contend with content blocking at some point in time, as content consumers: 53% of Internet users have tried to access content on social networks before, but found it to be blocked.

Out of the Internet users who share content (all types of content), 15% have received a message blocking their content before, i.e. 9% of Internet users. In detail:

- half of the blocked sharers received only one message from the platforms. On average, individuals sharing content have been blocked 4.85 times (with different content);
- 51% of the time, the messages received followed the posting of original works (i.e. content entirely authored by others), and 29% of mixed content.



More specifically, 11% of these “sharers” have received copyright-related blocking messages before, i.e. 6% of Internet users. Looking only at those whose audiovisual or video content had been blocked, the incidence rate was 4% (specific target studied in detail in the 2<sup>nd</sup> phase of the quantitative study).

2.3.4.3. – A well-managed contestation process.

Summary diagram – blocking and blocking contestations related to copyright issues

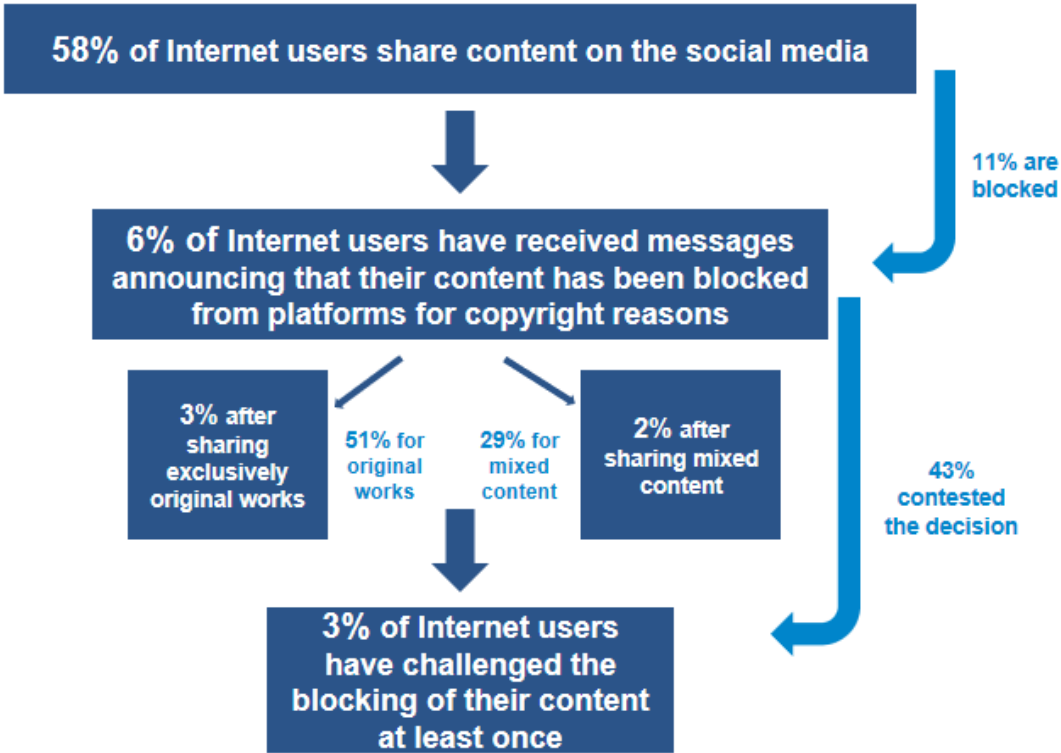


Figure 25

Source: OpinionWay study for Hadopi, 2019

Nearly half (43%) of blocked users contested the order to block their content and 27% of users even contested multiple blocks. All in all, 3% of Internet users have contested a blocking measure at some point.

The vast majority of those who were blocked stated that they understood the reason for which they received the message the first time: 67% immediately and 22% after seeking information. However, one-third (34%) of those who were blocked felt that the blocking measure was, overall, not warranted, half of them because it was an excerpt.

Generally speaking, while 39% of Internet users see the content blocking policies of social media to be “inappropriate”, this perception is shared by 49% of audio/video content sharing providers (+10 points) and especially by 75% of those sharing blocked content.

While users clearly got the message when blocked, they need more educational action and explanation from the platforms, so that they can also understand the legitimacy of the blocking action.

2.3.5. – Blocking instances related more to video content, are generally well understood and often uncontested, but users underline fear, complexity and even uselessness as reason not to contest.

One-third of internet users share audio and video content, while 58% shared at least one piece of owned content out of all those tested. The blocking of this content for copyright reasons concerns a comparable percentage of sharing Internet users: 13% have already had their audio or video content blocked (11% across all owned content), i.e. a total of 4% of Internet users.

2.3.5.1. – Analysis of blocking instances.

The study took a closer look at the most recent instance of blocking experienced by each of the users. First of all, it would appear that blocking occurs more frequently with posts containing videos: 75% of the Internet users surveyed on their most recent experience of blocking reported that it pertained to video content, compared with 31% for whom the content involved was audio.

Overall, around 3% of Internet users attempting to post videos were blocked by their social media or content sharing platform, while 1% had tried to post audio before being blocked.

**Content affected by most recent blocking action – database of blocked sharers of audio or video content**

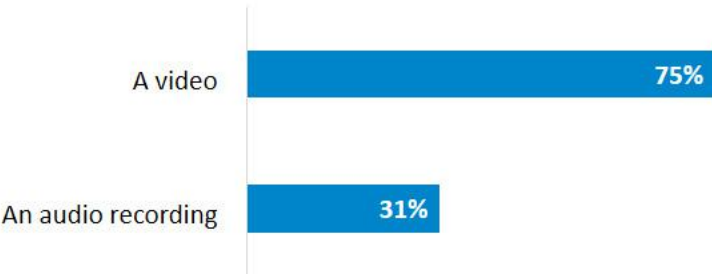


Figure 26

Source: OpinionWay study for Hadopi, 2019

Users were equally likely to have experienced blocking of their posts on Facebook or YouTube (42% and 37% respectively), while 13% of them had most recently experienced blocking on Instagram. Content can be shared on multiple platforms, and one-third of those having been blocked on one medium were also blocked by another social media (30%).

In contrast, content blocking on Twitter, Dailymotion and Reddit remains relatively limited, a statistic that could be ascribed to multiple factors, such as the lower proportion of users putting these platforms to use for content sharing, or, when relevant, the lack of identification technologies implemented by the said platforms (as is the case with Twitter).

**Platforms having sought the most recent blocking action – database of blocked sharers of audio or video content**

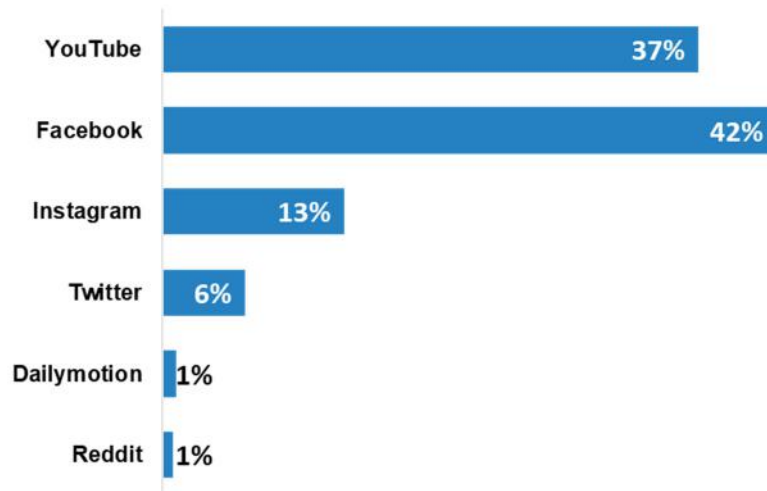


Figure 27

Source: OpinionWay study for Hadopi, 2019

The duration of the sequences affected by the block is relatively brief: half of the blocks involved content lasting less than one minute (47%). Only 16% of the blocks applied to content longer than 5 minutes.

### Duration of the sequence that led to the last blocking – database of blocked sharers of audio or video content

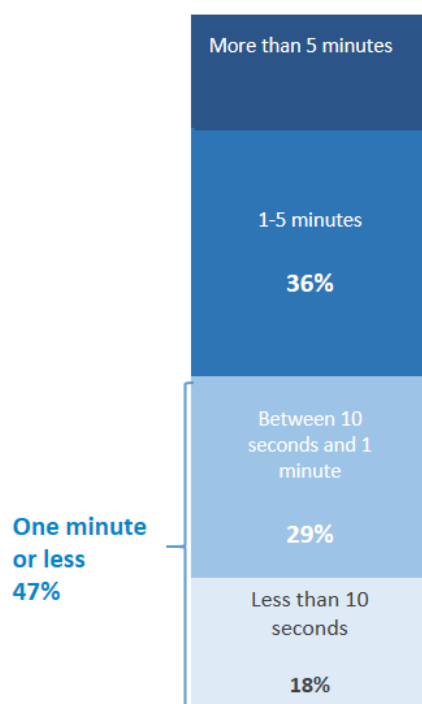


Figure 28

Source: OpinionWay study for Hadopi, 2019

#### 2.3.5.2. – Understanding and response of sharing parties in the face of measures.

The vast majority of Internet users who share audiovisual content understand the reasons for which the related audio and video content were blocked: 89% of blocked sharers say they understood the reason for which they last experienced a block, a rate that was the same for all sharers, regardless of the content shared. More specifically, 70% stated that they immediately understood the reason for which they received the blocking message, and 19% understood it after seeking further information.

However, 37% of them felt that the blocking decision was not warranted, a rate that also remained equal across all those surveyed on their blocking experiences overall (34%)

*“Thousands of people have used this song or the music, and they weren’t all blocked”*

*“Only a small part of the music was used”*

*“I generally share videos of non-recent songs, which you sometimes can’t find on other platforms. I don’t see the point in blocking them”.*

*“In the background you can hear music under copyright that was playing while I was making the video -- I didn't deliberately record the sound of the famous music!”*

**Perceived justifiability of the most recently received blocking message – database of blocked sharers of audio or video content**

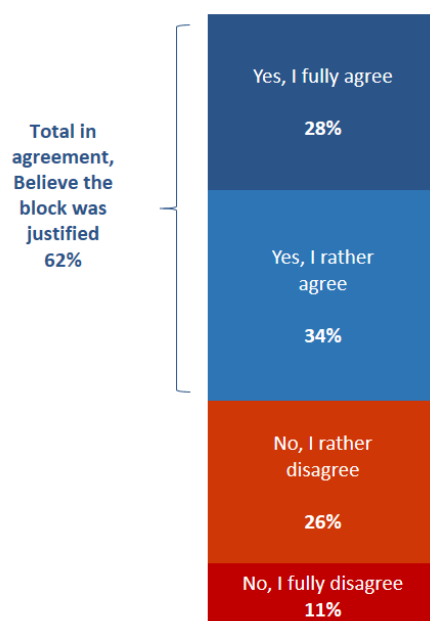


Figure 29

Source: OpinionWay study for Hadopi, 2019

Just over half of those who received a blocking message when sharing audio or video content (56%) disputed it, or about 2% of Internet users.

In the end, one-third of these “blocked” users said they had found a satisfactory solution following their complaint, either by having their content returned online, via an automatic reuploading mechanism by the platforms, or because they were convinced that the measure was valid.

### Contestation of last block – database of blocked sharers of audio or video content

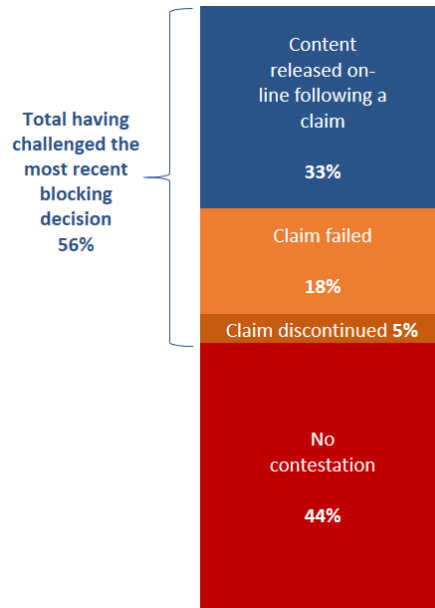


Figure 30

Source: OpinionWay study for Hadopi, 2019

A visual summary of this pathway is offered in the following diagram.

**Summary diagram – blocking and blocking contestations related to copyright issues**

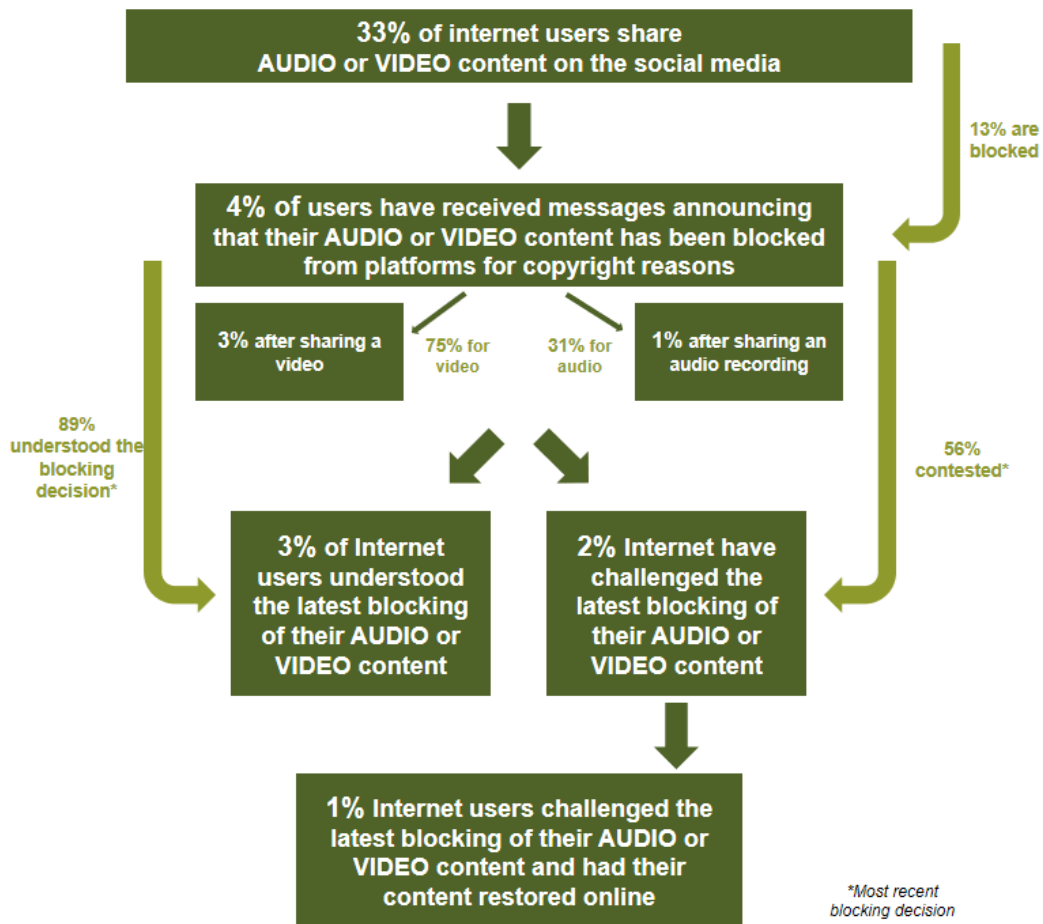


Figure 31

Source: OpinionWay study for Hadopi, 2019

Conversely, 44% of those blocked when sharing audio-visual content did not dispute the latest block they faced. They cite several reasons for this. First, one third stated that they did not see the point (37%), or more simply did not understand the reasons for the decision to block (30%).

Some of the blocked sharers deemed the situation complex: 20% referred to the process as complicated, 14% did not know whom to contact, 11% did not know how to do it, but most importantly almost one-fourth (23%) said they were “certain they would not prevail”.

Lastly, fear of having their account closed was the reason listed by 8% of those who did not dispute the last decision to block their content, and 5% of them referred to their fear of being ‘blacklisted’.

**Reasons for not contesting the last block – database of blocked audio or video sharers who did not contest the last instance of blocking on their content**

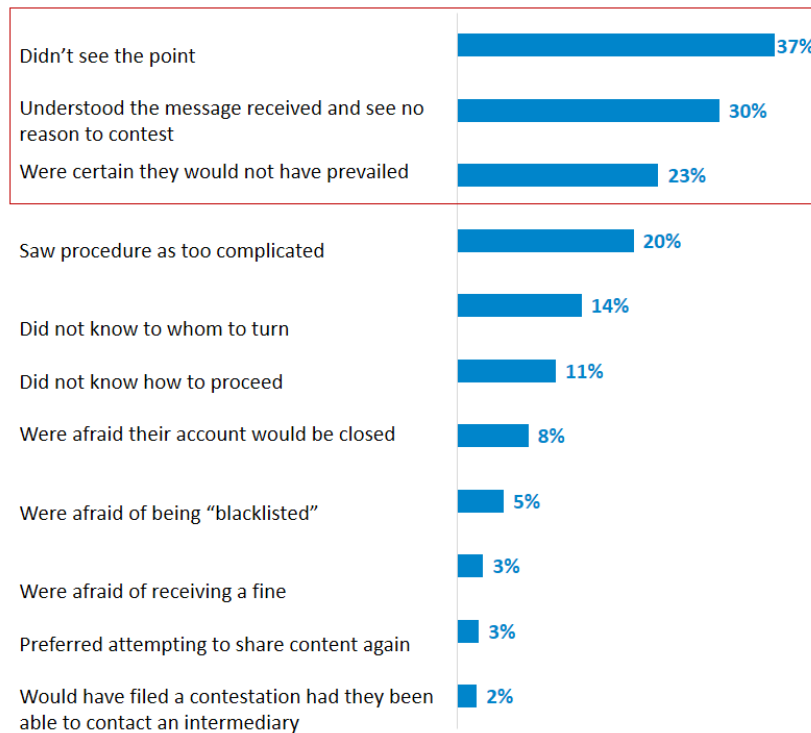


Figure 32

Source: OpinionWay study for Hadopi, 2019

Further to their content's being blocked, half of the sharers sought information about content sharing rules (47% of those whose audiovisual material was blocked).

However, it can be observed that a third (34%) of those Internet users whose most recent audio or video content was blocked wish to take measures to circumvent blockages on the platform.

To wit, 44% of the blocked Internet users looked for ways to use another platform that would be either more flexible on the issue of claims, or less respectful of copyright. This brings out the importance of having the means to assess the various technologies in question and of establishing a framework within which differences in the treatment of disputes can be substantiated and differences in the assessment of cases of legitimate exceptions or limitations to copyright can be remedied.



### Impact of blocks on content sharing practices – database of blocked sharers of audio or video content

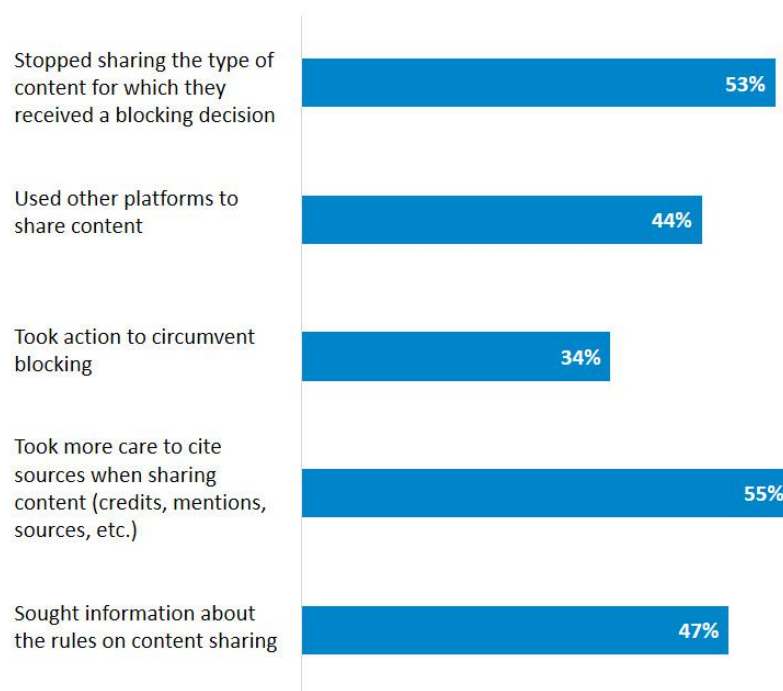


Figure 33

Source: OpinionWay study for Hadopi, 2019

Lastly, 55% of blocked Internet users stated that they were more careful about citing sources (credits, mentions, etc.) when sharing content, a response that demonstrates a problem in understanding the rules of authorisation for sharing copyrighted content, since citing sources does not mean that the rightful owner has authorised the content's use.

Overall, the fear of the consequences of a dispute, listed by 14% of the blocked who did not contest, and the absence of a clearly identified and neutral point of contact (16% did not know who to contact or would have liked a neutral intermediary to be present), combined with the need to find out about the rules for sharing content (47% of the blocked), seem symptomatic of a relative lack of clarity in the functioning of the platforms.

*"I didn't think I was doing anything illegal"*

*"Thousands of people have used this song or the music, and they weren't all blocked"*

*"I used copyrighted music and couldn't figure out how to flag it when posting my video"*

2.3.6. - Initially treated by platforms like any other users, though they also tend to be seen as rightholders, videographers remain in an ambivalent position with regard to recognition tools.

2.3.6.1. - *Initially viewed as ordinary users, videographers have had to deal with the limitations that recognition tools impose on their activities.*

Online sharing platforms have brought new life to the circle of creators by offering anyone the opportunity to create their own content and find an audience.

Through the diversity of their production and often personal tone, videographers, or “YouTubers”, have contributed to the platforms’ success. They have created new forms for a new audience. Platforms such as YouTube offer their users the possibility to monetise the content broadcast on their channels, if they choose to become “partners”. This status entitles them to share advertising revenues, in accordance with YouTube conditions, and more widely to enjoy a range of services that enable them to generate income (subscription to the channel, share in user's payment to appear separately on the on-line chat, etc.)<sup>38</sup>.

Videographers’ works, classified in the vast category of UGC content (“*User Generated Content*”), did not enjoy any particular protection advantage, even though, implementing a creative process and with the use of increasingly professional techniques, they naturally fall under the protection of copyright under ordinary law conditions.

Some videographers have thus come to see copyright, and *a fortiori* content recognition tools, with some ambivalence. Even though by uploading their videos on the platform, they transferred their exploitation rights, they were also faced with the enforcement of rights when their creations were based on the works of rightholders in more traditional sectors.

The situation proved to be particularly sensitive for videographers producing videos in the field of film criticism, parodies or documentaries, which were more likely to reuse protected content. The claim on the content by the original rightholder causes the videographer to: lose the monetisation revenues associated with the video, which are refunded in full to the rightholder who claimed the reused content; see the video blocked, if such is the rule set by the rightholder of the reused content; possibly even be subject to “strikes” that jeopardise the channel’s long-term future.

This particular sensitivity shown by videographers comes within a broader context of guarantee-seeking about the operating rules applied by platforms, for example transparency on the types of content that can be the subject of a “demonetisation” ruling due to the sensitivity of the content or, more generally, all remuneration rules<sup>39</sup>.

---

<sup>38</sup> See: “Generating revenue on YouTube” <https://support.google.com/youtube/answer/72857?hl=en>

<sup>39</sup> In addition to the recent creation in France of a Video Artist Guild, which the mission met, also of note is the creation in Germany of a group of videographers, called The YouTubers Union, which calls for greater transparency in the remuneration criteria applied to creations broadcast on the platform, in association with the (originally) metallurgy trade union IG Metall.

*2.3.6.2. - The recognised role of videographers in the platform economy has prompted YouTube to offer them certain functions for managing their creations.*

For YouTube, the appearance on the platform of new forms of content production and new creators, sometimes enjoying significant public renown, is an important component, which the platform has translated semantically by enshrining the concept of creator.

YouTube has also gradually taken their expectations more into account by providing them with tools to protect their content, albeit in a less developed form than Content ID, known as Copyright Match. In contrast to Content ID, its identification process does not focus on excerpts of protected content, and instead only the identical or near-identical copy of the content for which protection is requested. The tool is reserved for creators participating in YouTube Partner programme<sup>40</sup>.

Furthermore, in response to a request from videographers, YouTube has recently set up, in the case of so-called manual claims, a tool enabling the exact identification of the excerpt from the video that is the subject of the claim by the rights holder<sup>41</sup>. Videographers are thus able to better understand why their creation is in dispute, and if necessary, contest it, if they feel they have the grounds to do so.

*2.3.6.3. Videographers remain critical of what they experience as unfair treatment compared to rightholders protected by recognition tools.*

The new functionalities offered to videographers, as well as the decrease (in favour of partnerships with brands) in the share of monetization revenues in their revenues and their access to more traditional distribution channels, are in line with a relative abatement in the sensitivities expressed by videographers.

However, in general, the videographers interviewed by the mission wish to secure greater recognition for their creations, and specifically take aim at the constraints arising from the operation of content recognition tools and the way in which they are implemented.

Some representatives of the videographers met by the mission expressed their dissatisfaction with the application of the exceptions to copyright and related rights on platforms. Their criticism relates in particular to the application of the exceptions recognised by the Intellectual Property Code as pertains to short quotations and parody. As stated previously, content recognition tools, even if they can be configured in such a way as to offer a certain flexibility, particularly in terms of quoting excerpts, cannot by definition make the detailed assessments required for the proper application of exceptions,

---

<sup>40</sup> See: <https://support.google.com/youtube/answer/7648743?hl=en>

<sup>41</sup> See: <https://youtube-creators.googleblog.com/2019/07/better-tools-to-resolve-manual-Content-ID-claims.html>

particularly when it comes to parody. The videographers' criticism therefore pertains above all to cases of removals and blockages which they deem not justified.

Their criticism also extends to the platform's dispute resolution method, which does not ensure videographers an impartial decision but requires them to engage in dialogue with the rightholders, including when they feel that the latter does not take their invocation of the exception seriously enough. The time needed to deal with conflicts is also an extremely sensitive topic, as most monetisation revenues are received within 24 to 48 hours after the upload.

The videographers wonder whether mechanisms capable of establishing their good faith might be developed. They demand guarantees on the dialogue with the rightholders, refusing to be treated as though they were ordinary users, when the video shared might have been the result of significant investment on their part. The idea thus emerged over the course of the hearings with the mission that video creators offering guarantees of professionalism and good faith should be given special recognition, for example by being placed on a "white list" that would facilitate their reuse practices.

### 3. - Article 17 of the Directive on Copyright in the Digital Single Market makes content recognition tools central to the new balance still to be built.

Drafted and negotiated against the backdrop of the multiple expectations described above, Article 17 of the European Directive on Copyright in the Digital Single Market provides an innovative response, as it revamps the legal framework for sharing protected works and subject matter on platforms, and therefore the framework within which recognition tools are defined and implemented.

#### **What does Article 17 of Directive 2017/790 provide?**

**Article 17 defines the concept of online content-sharing service providers<sup>42</sup> and the regime applicable to these operators** who store and give the public access to a significant quantity of works (protected by copyright) and protected subject matter (protected by a related right) that are uploaded by their users (on the scope, see box below).

Article 17 provides that by giving the public access to this large number of protected works and subject matter, these service providers **perform acts of exploitation under copyright and related rights and therefore incur legal liability**, specifying that, when authorisations are issued to them, they also cover non-commercial users (Internet users seeking no profit in their use of the platform). In order to perform these acts, the services must **obtain an authorisation** from the rightholders. **If no authorisation is granted**, they shall be liable for unauthorised acts of communication to the public unless they demonstrate that they have **to ensure the unavailability of specific works and other subject matter on their service, they have made their “best efforts**, in accordance with high industry standards of professional diligence”, and based on the relevant and necessary information provided to them by rightholders, to disable access, remove and prevent the upload of unauthorised content.

Article 17 lays down a **high level of requirement for assessing these efforts**, while specifying that their intensity must take account, in light of the principle of proportionality, of factors such as the size of the service, the type of protected works and subject matter made available, the availability and cost of measures intended to combat the presence on sharing services of unauthorised protected works and subject matter.

**Lastly, Article 17 allows users to dispute the disabling of access to or removal of a protected work or subject matter that prevents the lawful use of that work or subject matter.** It provides that users must be able to assert the use of existing exceptions and limitations related to quotation, criticism and review as well as caricature, parody or pastiche. It requires service providers to set up an internal mechanism for handling complaints and the introduction by the Member States of a possible out-of-court appeal system for the user, without prejudice to a possible appeal to the court.

---

<sup>42</sup> The term “platforms” used below refers to this notion of “online content-sharing service providers” within the meaning of Article 17 of the Directive.

## **To which operators does Article 17 apply?**

**The concept of online content-sharing service provider refers, under Article 2 of the Directive, to “a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes”. Recital 62 states that this definition “should target only online services that play an important role on the online content market by competing with other online content services, such as online audio and video streaming services”.**

**The decisive criteria are therefore:**

- *the significant quantity of protected content made available to the public (audience of the service and number of protected files uploaded),*
- *the main objective or one of the main objectives of the service, which must be to store and offer the public access to this protected content,*
- *the role played by the platform in classifying and promoting the content,*
- *and the direct or indirect profit sought by the platform.*

**Subject to the decisions that will be taken by the competent authorities in the implementation of the texts transposing the Directive, the scope of this concept seems to cover, provided these conditions are met, social media focusing on the sharing of video or music content (YouTube, Soundcloud, Vimeo, Dailymotion, Tiktok, etc.), as well as more general social media that may give rise to very diverse content sharing (Facebook, Instagram, Twitter, Snapchat, etc.) or more targeted platforms (Twitch initially focused on video games, Pinterest or Flickr on images, Scribd or Calameo on written content, or even ResearchGate for scientific articles) and blog sites (Tumblr, Overblog, etc.). As for messaging applications (WhatsApp, Messenger, etc.), they could only be covered if it was considered that giving the public access to protected content is their main objective or one of their main objectives.**

**A temporary derogation is provided for services made available to the public within the European Union for less than three years and with an annual turnover below EUR 10 million. This regime differs depending on whether the number of unique visitors to the site is less than or more than EUR 5 million at the European Union level.**

*The concept of online content-sharing service provider defined by the Directive (art. 2) does not apply to non-profit online encyclopaedias, non-profit educational and scientific directories, open-source software development and sharing platforms, providers of electronic communications services within the meaning of Directive (EU) 2018/1972, providers of online marketplaces, cloud services between companies and cloud services that allow users to upload content for their own use .*

*Similarly, recital 62 provides that, “in order to ensure a high level of copyright protection, the liability exemption mechanism (...) should not apply to service providers the main purpose of which is to engage in or facilitate copyright piracy”.*

Sharing platforms thus enjoy a clearer definition of the nature of their activity with regard to the prerogatives granted to holders of copyright and related rights by Article 3 of the 2001 Directive on copyright and related rights<sup>43</sup>. It is now clearly stated that by giving access to the public to protected content, they carry out an act of communication to the public within the meaning of Article 3 of Directive 2001/29, .

In addition, they are assigned a very different regime to the one in which they appeared, characterised by the status of the host originating, in the United States, from the *Digital Millennium Copyright Act* and, in Europe, from the Directive on e-Commerce<sup>44</sup>.

It is in the light of these elements that the role of recognition tools is redefined. Until now, they had been developed by the platforms in a manner presented as purely voluntary. This context determined in depth both the functionalities offered by these tools and their mode of governance, which were ultimately *decided unilaterally by the platforms*.

With Article 17 of the European Directive, and while platforms are clearly recognised as carrying out acts of commercial use of copyright and related rights subject to authorisation, the traceability of these acts of exploitation and the effectiveness of the rights involved are no longer an option, but indeed firmly imposed legal obligations. In this perspective, recognition tools will be called upon to play a new role. No longer will they be able to remain purely technical solutions determined by platforms and whose operation is not transparent to users and rightholders. They are destined to play a central role in the new balances to be built.

### 3.1. Content recognition tools are an essential aspect of the implementation of Article 17, which requires actors to come up to standard in this respect.

While, in the final version, Article 17 of the Directive does not contain an explicit reference to content recognition tools, these tools nevertheless appear to be a key component in its implementation, in order to ensure the blocking or removal of unauthorised content. They may also find a place, in the event of authorisation issued by rightholders, in ensuring the identification of the content used on the platforms. In both cases, the existing recognition tools, and first and foremost the audio and video fingerprint recognition algorithms, are, in view of their deployment and performance, destined to serve as a reference point.

---

<sup>43</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

<sup>44</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market.

3.1.1. - The blocking and removal procedures provided for in Article 17 will be based on the implementation of content recognition tools, at least for audio and video content.

The platforms covered by Article 17 must, as Paragraph 1 of the said article specifies, obtain an authorisation *“for instance by concluding a licensing agreement, in order to communicate to the public or make available to the public works or other subject matter”*. Recital 61 states that: *“Those licensing agreements should be fair and keep a reasonable balance between both parties. Rightholders should receive appropriate remuneration for the use of their works or other subject matter. However, as contractual freedom should not be affected by those provisions, rightholders should not be obliged to give an authorisation or to conclude licensing agreements.”*

In the absence of authorisation, platforms are liable for any unauthorised acts of communication to the public, unless they demonstrate not only that they have made their best efforts to obtain an authorisation, but also that they have made their *“best efforts, in accordance with high industry standards of professional diligence, to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information”*. In addition, they must act promptly, upon receipt of a sufficiently substantiated notification from the rightholders, to block access to the works and other protected subject matter that are the object of the notification or to remove them from their websites, and, once again, make *“their best efforts to prevent the future uploads”*.

This notion of “best efforts”, which is introduced by the Directive in the event that the platform has not been granted authorisation to store and give access to protected content, therefore serves the objective of combating the presence of unauthorised content on the platforms. It therefore has a dual dimension: on the one hand, preventing the sharing of unauthorised content on the platform and, on the other, when certain content has been removed on notification of a beneficiary, preventing it from being uploaded again in the future. As mentioned in Article 17, paragraph 9, dealing with complaints and appeals, it therefore results in decisions to block access to works or other protected subject matter uploaded by users or in decisions to remove such content.

Such blocking or removal decisions may relate to content for which the rightholders have not granted any authorisation to the platform, but also content for which the rightholders have granted certain authorisations, but which is not covered by this authorisation, which is a common scenario. A rightholder who authorises the presence of his catalogue on a platform very often also has reasons to exclude certain content from the scope of the authorisation, if only for example phonograms until their official publication date. Consequently, even rightholders who have granted authorisations may be required to provide the relevant and necessary information to have certain content removed and blocked.

The provision of relevant and necessary information by the holders on the works and other specific protected subject matter conditions the possibility of holding the platforms liable for not having provided their best efforts to guarantee the unavailability of the content. As stated in recital 66: *“Where rightholders do not provide online content-sharing service providers with the relevant and*



*necessary information on their specific works or other subject matter, or where no notification concerning the disabling of access to, or the removal of, specific unauthorised works or other subject matter has been provided by rightholders, and, as a result, those service providers cannot make their best efforts to avoid the availability of unauthorised content on their services, in accordance with high industry standards of professional diligence, such service providers should not be liable for unauthorised acts of communication to the public or of making available to the public of such unidentified works or other subject matter”.*

The rightholders must provide the platforms with such relevant and necessary information, pursuant to recital 66, *“taking into account, among other factors, the size of the rightholders and the type of their works and other subject matter”*. They must therefore cover the specific content of which the unavailability must be guaranteed by blocking and removal measures.

By referring to the *“high industry standards of professional diligence,”*, the Directive requires that the best efforts be defined not on the basis of a theoretical approach, but on the basis of the existing state of the art, referring to the most efficient developments. It does not prescribe any particular technology, but it makes the performance of existing technologies and the measures implemented by relevant platforms a crucial benchmark for defining the liability regime to be applied. Recital 66 thus specifies that *“best practices in the sector”* must be taken into account: *“When assessing whether an online content-sharing service provider has made its best efforts in accordance with the high industry standards of professional diligence, account should be taken of whether the service provider has taken all the steps that would be taken by a diligent operator to achieve the result of preventing the availability of unauthorised works or other subject matter on its website, taking into account best industry practices and the effectiveness of the steps taken in light of all relevant factors and developments, as well as the principle of proportionality”*.

It is with this in mind that existing content recognition tools, and in particular fingerprint recognition algorithms for audio and video content deployed on certain platforms, appear to be an essential reference point in the implementation of Article 17.

In the current state of the art, fingerprint recognition tools are the only systems deployed on a large scale to ensure the unavailability of content shared without authorisation. They operate on the basis of relevant and necessary information provided by the relevant rightholders on specific content (either fingerprints or the content itself). They enable unauthorised shared content to be blocked or removed, with an established degree of effectiveness, even though the constant improvements visible today demonstrate that effectiveness is a concept always subject to discussion.

As for the other content recognition tools described above, based in particular on hashing, the use of metadata, watermarking and the contributions of artificial intelligence, they cannot, given their state of deployment and (for some of them) their inherent limitations, have such a central place in the assessment of the *“best efforts”* provided for by Article 17. They must, however, be taken into account when defining the best efforts, especially in those sectors where the platforms have not deployed fingerprinting systems and where the Directive lays out, in a sense, a blank page that is yet to be

written. Above all, it is important to ensure that all technologies remain taken into account in the dynamic assessment which the notion of “best efforts” will require.

While fingerprinting systems play a central part in assessing the best efforts within the meaning of the Directive, this clearly does not imply that all the functionalities currently deployed on platforms become *ipso facto* mandatory. It is first and foremost as recognition tools enabling blocking and removal that they become an essential reference in the implementation of Article 17. However, by requiring platforms to collect permission from rightholders, Article 17 could also affect the role and scope of recognition tools in other ways.

### 3.1.2. - For content authorised by rightholders, tools will also be needed to identify acts of exploitation

In addition blocking or removing of unauthorised content, existing content recognition tools may also be used to measure and trace the authorised acts of commercial use of content.

Since they carry out acts of exploitation of copyright and related rights, and can not claim to be mere hosting service providers, the platforms have to report these acts to the rightholders who have granted them the authorisations to do so. This is provided for in paragraph 8 of Article 17 which states that: *“Member States shall provide that online content-sharing service providers provide rightholders, (...) where licensing agreements are concluded between service providers and rightholders, information on the use of content covered by the agreements.”*

The provision to rightholders of information on the use of content covered by an authorisation and shared by users is only referred to in general terms in the Directive. In contrast with what it states about the “best efforts” described above, the Directive does not set standards by reference to existing best practices. This area is, moreover, logically a matter of discussion between the platform and the rightholders who grant it authorisation.

However, given the recognition tools currently deployed by the platforms in terms of audio and video content and the rules that will apply in terms of unauthorised content, it will make sense to use these recognition tools to identify acts of exploitation and to report information to rightholders, or even to calculate the rights to be distributed.

In this case, the transparency obligations specified by Recital 68 of the Directive should apply, on the dual basis of the Directive, which introduces a minimum set of rules in this area, and contractual agreements, which may contain additional provisions: *“Online content-sharing service providers should be transparent with rightholders with regard to the steps taken in the context of cooperation. As various actions could be undertaken by online content-sharing service providers, they should provide rightholders, at the request of rightholders, with adequate information on the type of actions undertaken and the way in which they are undertaken. Such information should be sufficiently specific to provide enough transparency to rightholders, without affecting business secrets of online content-sharing service providers. Service providers should, however, not be required to provide rightholders with detailed and individualised information for each work or other subject matter identified. That*

*should be without prejudice to contractual arrangements, which could contain more specific provisions on the information to be provided where agreements are concluded between service providers and rightholders.”*

Thus, it is clear that the three main functions assigned to recognition tools currently deployed on platforms (the transmission of information, the monetization of content through the sharing of advertising revenues and the blocking of unauthorized content) are not equally affected by the provisions of Article 17. Through the notion of best efforts for platforms with regard to unauthorised content, it is very clearly the blocking function that is directly influenced by the requirements of Article 17. However, the function of transmitting information on uses is also mentioned. As for the function played to enable the monetisation of content, it can be considered as being addressed by the provisions on transparency (Article 17(8) and recital 68).

All in all, it is clear that the implementation of the Directive can only give a central role to existing recognition tools, and in particular to the fingerprinting systems deployed for the recognition of audio and video content, in assessing the best efforts of the platforms in terms of removing or blocking and preventing the re-posting of content online. In the context of the negotiations between rightholders and platforms, there will be a strong drive to ensure that these recognition tools are also used to provide information on the uses made of authorised content, and therefore to calculate the remuneration due for these uses.

### 3.1.3. - As a result, platforms will need to make efforts to ensure they are up to standard on the protection of rights.

By clarifying the legal regime of sharing platforms, Article 17 first and foremost contributes to unifying the law applicable to competing operators on the same market. These service providers have hitherto claimed to fall under the host status, even though they were aware that their activity was under risk of a different legal qualification by the jurisdictions. By providing for best efforts defined by reference to high industry standards, Article 17 helps to level competitive conditions and, ultimately, to clean up the market overall. As stated above, while recognition tools have been deployed on a massive scale by the most widely used platforms, real disparities remain to date. Henceforth, the varying degrees of laxity seen on the market regarding the presence of unauthorised content should not constitute a differentiating factor in the competition between sharing platforms.

The logic underlying Article 17 should also tend to harmonise the effectiveness of the recognition tools deployed. The best practices expected from platforms are aimed first and foremost at robust recognition, so as to ensure the unavailability of unauthorised content. The performance harmonisation effect is expected to also apply to the sharpness of recognition, so as to avoid false positives and unjustified blocking practices. Lastly, it is logical, in view of the transparency obligation placed on platforms in their contractual relations with right holders, that the management functionalities offered to rightholders should also be applied in order to identify the uses covered by these agreements.

Similarly, the notion of best efforts provided for by Article 17 will no longer allow sharing services to modulate at their discretion the way recognition tools are implemented on the different segments of their offer. The unilateral nature of the implementation of existing content recognition tools may have given rise to the suspicion that some parts of the platforms were not subject to these tools in the same way as others. Such conjecture no longer appears relevant for YouTube channels managed and held by *networks* (or *Multi Channel networks*) which, according to the testimonies gathered by the mission, are now subject to Content ID's rules in the same way as any other channel. That a suspicion of differential treatment may have existed for a long time is nevertheless significant. In addition, it would appear that content uploaded to YouTube by the so-called "preferred partners" is not always subject to the application of Content ID, which in many cases is understandable (for example, content uploaded by a partner television channel may be presumed not to pose any difficulties) but may in some respects be worth discussing (for example, the absence of recognition by Content ID is certainly detrimental to certain rightholders whose rights should in any case be protected, such as music authors' and composers).

Similarly, the Directive, by requiring that platforms obtain an authorisation from rightholders and by providing that they use, in order not to be held liable, their best efforts to ensure the unavailability of unauthorised content, prohibits them from choosing at their complete discretion the partners whose authorisations they seek and those to whom they offer access to their recognition tools. This aligns with the central inspiration of Article 17: rightholders protection is no longer a mere option and the provision of effective tools is no longer a facility which they can grant only to partners they consider worthy of it. This does not mean, however, that Article 17 requires absolute exhaustiveness with regard to authorisation agreements and the scope of application of recognition tools. Firstly, because the platforms are not bound, where authorisations are concerned, by a performance obligation, but by an obligation of means, reflected in the notion of best efforts to obtain an authorisation referred to in a) of paragraph 4. In addition, the best efforts to guarantee the unavailability of unauthorised content are assessed in the light of such factors as the number of content items concerned and the principle of proportionality. Lastly, the platform's liability for unauthorised content is only possible if the relevant and necessary information has been provided by the rightholder.

In order to operate without incurring liability for unauthorised content, platforms are not required to hold authorisations for all the content to which they offer access. In contrast, they must make their best efforts to obtain authorisations, particularly from rightholders whose content they offer to the public the most, and without refusing to enter negotiations with the rightholders who request it. Similarly, the best efforts to ensure the unavailability of specific unauthorised content are assessed only on the basis of the relevant and necessary information provided to them by the rightholders.

Finally, another aspect of this general upgrade of rights protection, Article 17 states that audio and video are no longer the only sectors in which rightholders can sign agreements with platforms and benefit from tools that effectively guarantee the unavailability of unauthorised content. For reasons relating both to the significant presence of their content on the platforms and to their bargaining power, in particular in the United States, the country of origin of most platforms, up to now, it was only the rightholders (in particular producers and broadcasters, but also certain authors and

publishers) of the music and audiovisual sectors that benefited from the recognition tools deployed by the platforms. From now on, effective protection must also be provided to all the rightholders protected according to Article 3 of Directive 2001/29 and whose content is shared on the platforms. This could apply, naturally depending on the platforms, to the rightholders of still images (visual arts authors, photographers, photo agencies and press agencies), written content (authors and publishers of books and newspapers) or even video games, etc.

Depending on the actual presence of this content on the platforms and the decisions taken by rightholders, Article 17 therefore paves the way for agreements to be negotiated, enabling the sharing of all protected content on the platforms and provides the definition of the best efforts expected of them to prevent the availability of unauthorised content.

### 3.2. The approach adopted for the Directive makes it possible to address many of the concerns raised during its discussion.

While Article 17 proved highly controversial during its negotiation, both in terms of principles and of technical feasibility and, the approach adopted for the Directive, on the contrary, makes its implementation an opportunity for real progress by all actors in their deployment of content recognition tools.

#### 3.2.1. The approach adopted for the Directive is based on a pragmatic and proportionate implementation of recognition tools.

Article 17, without imposing any technology in particular, focuses on the objectives to be achieved, which are to ensure the unavailability of unauthorised content and to allow authorisations to operate when they are issued by rightholders. This goal-oriented approach has the advantage of being able to withstand the passage of time. By referring to the existing state of the art, it allows immediate implementation of the Directive's objectives, which will be achieved in particular, for audio and video content, by referring to the performance of the fingerprinting systems already deployed by many platforms. However, none of the Directive's provisions lock the actors into a given state of the art in technology. It will be up to them, as well as the public authorities involved in the implementation of the Directive in the Member States and at the EU level (ultimately the competent judicial authorities), to update the assessment of the best efforts required of the platforms.

Article 17 of the Directive also refers to the application not only of a high industry standard, but also of the principle of proportionality in assessing the best efforts of the platforms. In paragraph 5, it provides that: *“In determining whether the service provider has complied with its obligations under paragraph 4, and in light of the principle of proportionality, the following elements, among others, shall be taken into account: (a) the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service; and (b) the availability of suitable and effective means and their cost for service providers”*. This approach implies that best efforts do not

consist in the implementation of tools that are either not operational or that might suffer from constraints not in line with the objectives sought.

In particular, while Article 17 implies new protection against the provision of unauthorised content for rightholders who have not previously benefited from recognition systems deployed on platforms, it also provides that the best efforts expected of platforms must take into account the features specific to each sector. Recital 66 of the Directive thus states that: *“Different means to avoid the availability of unauthorised copyright-protected content could be appropriate and proportionate depending on the type of content, and, therefore, it cannot be excluded that in some cases availability of unauthorised content can only be avoided upon notification of rightholders. Any steps taken by service providers should be effective with regard to the objectives pursued but should not go beyond what is necessary to achieve the objective of avoiding and discontinuing the availability of unauthorised works and other subject matter.”*

In this sense, while fingerprinting systems are an essential reference point in determining the best efforts of the platforms in terms of audio and video content, since they are already deployed on a large scale, it remains to be determined the content of the best efforts, and therefore the appropriate recognition tools, with regard to other types of content, such as photographs or texts.

To achieve a smooth and effective implementation of Article 17, the European legislator also requires cooperation between the actors. Paragraph 10 of Article 17 thus provides as follows: *“As of 6 June 2019, the Commission is organising, in cooperation with Member States, stakeholder dialogues to discuss best practices for cooperation between online content-sharing service providers and rightholders. The Commission shall, in consultation with online content-sharing service providers, rightholders, users' organisations and other relevant stakeholders, and taking into account the results of the stakeholder dialogues, issue guidance on the application of this Article, in particular regarding the cooperation referred to in paragraph 4. When discussing best practices, special account shall be taken, among other things, of the need to balance fundamental rights and of the use of exceptions and limitations”*.

All in all, it is clear that the approach adopted by Article 17 is in no way out of touch with current practices, locked in a given state of the art or lacking in balance; rather, it is the result of a compromise between the many considerations involved, and it is well suited to make it possible to strike a fine balance between them.

3.2.2. - Article 17 provides a new legal framework for content recognition tools, the practical importance of which was, until now, equalled only by the lack of transparency.

While many of the criticisms levelled at Article 17 by its opponents focused on content recognition tools (e.g., the campaign against “upload filters”), it is striking to see that these criticisms seemed to ignore the already massive presence of these tools on the most frequently used platforms, whether to identify protected content or for commercial policy reasons. By opposing Article 17 on these grounds,

such critics thus chose to perpetuate the very situation against which they argued, denying any possibility of recognising, and thereby regulating, an already massive reality. Apparently; the recognition tools implemented by platforms in a largely unilateral and, in many respects, discretionary and opaque manner<sup>45</sup> were for the opponents of Article 17 preferred over a legislative approach that aims at defining the legitimate expectations which these tools address and set out the principles with which they must comply. As if filtering by a platform was in principle preferable to the approach intended by the European legislator, despite the guarantees and balances that it involves...

Yet Article 17 provides, to the contrary, that the practices of platforms under best efforts requirement placed on them to guarantee the unavailability of unauthorised content should reflect greater transparency (term expressly used in recital 68).

In relation to rightholders, paragraph 8 of Article 17 thus provides that: *“Member States shall provide that online content-sharing service providers provide rightholders, at their request, with adequate information on the functioning of their practices with regard to the cooperation referred to in paragraph 4 and, where licensing agreements are concluded between service providers and rightholders, information on the use of content covered by the agreements.”*

With regard to users and all interested parties, paragraph 10 of Article 17, which concerns the dialogue to be organised between stakeholders by the European Commission before issuing its guidance, provides that: *“For the purpose of the stakeholder dialogues, users' organisations shall have access to adequate information from online content-sharing service providers on the functioning of their practices with regard to paragraph 4”* (relating to cooperation between platforms and rightholders for the removal and blocking of unauthorised content).

As explained above, however, the content recognition tools deployed on the platforms were not previously subject to any obligation of transparency, and tended, quite to the contrary, to be covered by under confidentiality agreements (*“non-disclosure agreements”*) imposed by the platforms. Born in a context of negotiation on uneven footing with rightholders, wherein host status was invoked by platforms, they were probably better known to the most powerful international rightholders. For a large number of rightholders, however, they remained largely black boxes in terms of how they were implemented and the completeness of their results. The transparency obligation provided for by the Directive, both in terms of practices and in terms of use of content, is therefore a critical aspect of its implementation. It should cover the implementation perimeter of content recognition tools, their possible limitations or defaults as well as the precise manner in which they are applied to the content that is stored by the platforms (as opposed to the uploaded content). As for users, they agreed to the application of content recognition tools by giving their mandatory consent to the general terms and conditions of use but were largely unaware of the the implications of this consent. Videographers, who

---

<sup>45</sup> Even though the unilateral manner in which the existing recognition tools have been deployed and the absence of any obligation of transparency are features common to all platforms, it should be noted that YouTube successfully distinguishes itself from other services by a real effort to explain how Content ID works and by providing users and rightholders with interfaces that enable them to fine-tune their practices.

were often quite directly dependent on the parameters of these recognition tools for the commercial gain they could derive from their activity, have also largely felt a lack of transparency on this aspect.

While it remains to be seen how the logic of increased transparency will be implemented by the Directive, it remains certain that the move in this direction will, by its principle, address widespread expectations expressed by the stakeholders.

### 3.2.3. - Article 17 by no means sets the stage for a single dominant player and instead lends itself to a variety of models in its implementation.

Another of the recurring criticisms aimed at Article 17 involved describing it as setting requirements that can only be met by very few actors with disproportionate financial resources. For example, it was argued that Article 17 created such a barrier to entry for emerging platforms that it was in fact a competitive advantage for YouTube (in view of the advance often recognized to Content ID) and, to a lesser extent, Facebook (which developed Rights Manager for the same purpose). While this criticism does deserve serious consideration, it fails to convince.

This criticism was fuelled by Google's recurrent references to the investments needed for the development and continuous improvement of Content ID. In its report, *How Google fights piracy 2018*<sup>46</sup>, Google states that since 2007, it has invested more than \$100 million in Content ID, including in terms of human resources and computer programming capabilities. This figure, incidentally raised by \$40 million over a period of just two years<sup>47</sup>, was abundantly quoted in the public debate around Article 17.

These references to the amount invested rightly raises the question of the costs required of platforms to set up an efficient content recognition tool. In the case of fingerprinting systems, the basic functionality, which is the creation of a fingerprint database and the application of a recognition algorithm to all uploaded content as well as periodically on the content which is stored, is not enough to ensure the effectiveness of the recognition process on its own. New features are regularly requested, for instance real-time fingerprint generation and content recognition, needed in order to combat the reuse of content broadcast *live* on the platforms, in particular sporting events. Above all, it can be noted that tools like Content ID are regularly updated (approximately every 6 months) to ensure greater effectiveness.

However, it would not be reasonable, on that mere basis,, to stop requiring that platforms step up their efforts to ensure that rights are respected.

First of all, it should be noted that the amount cited by Google is unverifiable and thus must be seen in perspective, in light of the period covered (more than 10 years) and the overall magnitude of

---

<sup>46</sup> [https://www.blog.google/documents/27/How\\_Google\\_Fights\\_Piracy\\_2018.pdf](https://www.blog.google/documents/27/How_Google_Fights_Piracy_2018.pdf)

<sup>47</sup> It was estimated at \$60 million in the *How Google fights Piracy* report published on 13 July 2016: <https://blog.google/outreach-initiatives/public-policy/continuing-to-create-value-while/>



investment made by a company like Google. It is also noted here that Facebook, meanwhile, implemented a fingerprinting system in a relatively short period without alleging comparable investments. The platform Dailymotion has likewise played a pioneering role in this area, using the technologies of Audible Magic and Ina (INA-Signature), obviously without having to consent to investments on the scale referred to by Google.

As stated above, content recognition on platforms is far from being limited to the tools developed by YouTube and Facebook internally (in its entirety or, for Facebook, partially).. In the field of music, the International Federation of the Phonographic Industry (IFPI) counts 43 providers offering recognition services and equipped with adequate databases. Not only Audible Magic, whose solution is deployed on multiple sharing platforms<sup>48</sup>, but also many of its competitors are able to meet the platforms' needs.

Analysis of current practices in the digital distribution of music shows content recognition on sharing platforms to be using technologies similar to those implemented for other purposes, for example for the notifications addressed to platforms engaged in mass illegal action, or for the analysis of music broadcast in public places or in the media. The market for content recognition technologies specific to the music industry is by no means lacking in very active actors, each having built up the databases of tens of millions of titles needed to protect music rights on platforms. Thus, if any questions remain as to the availability of content recognition technology solutions in some sectors, it is not the case as far as music rights are concerned.

Moreover, in the video and still image sectors, the existence of effective recognition technologies does not need further demonstration. A number of patented innovations are in the public domain or about to enter it<sup>49</sup>. While updating technologies likely does require real investment, it would probably be excessive to say that it is economically unrealistic.

In reality, it is rather the creation and updating of a sufficiently rich fingerprint base, particularly in the video field, that seems to be the most significant challenge to address in terms of content recognition. Without a doubt, YouTube and Facebook, actors with a massive and global audience, have a real lead in this area: it is difficult to imagine rightholders keen on securing protection for their own rights not taking the necessary action with such important actors. Conversely, for a platform such as Dailymotion, the creation of a relevant database is a major challenge: as things stand, French rightholders, those of certain European countries and international rightholders attached to full protection for their rights feed the platform's database, but, the database can hardly claim to provide exhaustive coverage of the video content which, in view of its value, should be protected.

Despite these challenges, solutions can already be found on the market for platforms wishing to set up a content recognition tool, including for video. As an illustration, Audible Magic's solution is

---

<sup>48</sup> According to the information provided by Audible Magic in September 2019, its automatic content recognition solutions have been deployed in particular on the following sharing services: Facebook, Instagram, Soundcloud, Dailymotion, Tiktok, Twitch, VK (Vkontakte).

<sup>49</sup> This is the case of the patent held by the University of British Columbia on SIFT (*Scale Invariant Feature Transform*) a technology described by experts as central to the definition of subject matter recognition algorithms, available under a non-exclusive license and set to enter the public domain in the United States and Canada (the only countries where it is not yet in the public domain) in 2020.

deployed on multiple major platforms not only for music content but also for video content: according to the figures provided by the company, activated fingerprints today protect more than 140,000 rightholders (music producers and publishers, film and audiovisual producers and broadcasters) from more than 140 countries (with the addition of 250,000 new titles each month). Similarly, the INA-Signature technology developed by the Ina has long been implemented by Dailymotion and is available to be provided to other platforms: the deployment of this technology has played a pioneering role, both in demonstrating the large-scale feasibility of fingerprinting systems and their development (in particular, real-time generation of fingerprints applicable to “live” content) and enjoys real renown at the international level<sup>50</sup>. Many other providers offer fingerprinting services aimed at protecting video content<sup>51</sup>.

Other innovative solutions exist or are in development. For instance, Qwant is considering a model for the generation of fingerprints by a decentralised solution open to a range of platforms. The start-up Pex reports that it has created a database by indexing and referencing close to 40 of the most popular platforms, and by associating fingerprints with them using the metadata associated with indexed content, which forms a particularly rich fingerprint database.

The elements detailed above (see 2.1.3) on the fees charged by recognition solutions providers suggest that this factor should not be insurmountable for platforms, the youngest of which can, moreover, in their first three years of operation, benefit from the special regime described in paragraph 6 of Article 17.

Above all, the flexibility inherent in the approach of Article 17 guarantees that platforms incur their liability for unauthorised content only within the limits of the due diligence carried out by the rightholders by providing the relevant and necessary information. Thus, whatever the limitations of the market’s existing tools, including with regard to the wealth of fingerprint databases, they cannot invalidate the approach adopted by Article 17 since, by definition, it imposes only what is possible.

Lastly, it is clear that the implementation of Article 17 will itself stimulate the market for recognition tools so as to respond to the needs of the platforms with regard to the best efforts expected of them. During its hearings, the mission noted the dynamism of the service offering in this area.

---

<sup>50</sup> In April 2018, the INA was commended by an *Emmy Award for Technology and Engineering* from the United States *National Academy of Television Arts and Sciences* (NATAS), in the category “*Video Identification Technology to protect content value and copyright*”.

<sup>51</sup> To illustrate, the *Emmy Award for Technology and Engineering* awarded to the Ina in 2018 was shared by six recipients: in addition to the Ina, YouTube and Audible Magic, Vobile (a company based in the USA), Civolution (a technology resulting from the exploitation of patents initially held by Royal Philips Electronics) and FriendMTS (a British company) were also commended. See [http://emmyonline.com/tech\\_69th\\_recipients](http://emmyonline.com/tech_69th_recipients).

3.3. - Article 17 calls for the definition of a concerted and differentiated approach when it comes to content other than fingerprintable audio and video.

While the principle of rightholders' authorisation laid down in Article 17 concerns all creative sectors the content of which is shared on platforms, it requires the definition of modalities that can be differentiated between these sectors. Article 17 and the recitals of the Directive explicitly refer to the diversity of situations from sector to sector, and therefore the variety of responses which they require. The best efforts provided by Article 17.4.b do not necessarily involve the implementation across all industries of such fingerprinting systems as currently used for audio and video content, but rather require that actors seek out solutions suited to the current state of the art and the features specific to their sector. They may therefore resort to a wide range of solutions, on the basis of those presented in the first part of the present report.

The solutions used by platforms to carry out their best efforts under Article 17.4.b will need to be assessed on a case by case basis by each platform in accordance with its characteristics. For every category of relevant rights, they will hinge upon the available technologies, their performance and their limitations but also the nature and scale of sharing practices observed. The best efforts under Article 17.4.b imply, in order to ensure the unavailability of unauthorised content, the prevention of uploading of specific works and objects, which calls for a high degree of performance in terms of recognition. Therefore, recital 66 of the Directive states that :*"it cannot be excluded that in some cases availability of unauthorised content can only be avoided upon notification of rightholders"*.

In such cases, sharing service providers should at least do their utmost to make it possible for rightholders to search their databases in order to detect unauthorised content and notify them to remove it. This implies that online sharing platforms should do away with large-scale metadata removal practices that are still prevalent, especially in the case of photographs. These practices hinder the search for unauthorised content and are in no way justifiable in view of the protection provided for by Article 17. A further beneficial step in this context would be the definition by platforms and rightholders of joint protocols dealing with unauthorised content search.

### 3.3.1. – Photography and Visual arts.

The principle of rightholders' authorisation laid down by Article 17 for the communication to the public on online sharing platforms of protected works covers the field of photography and visual arts (plastic arts, design, architecture) as well as other sectors. . This clearly includes image sharing platforms (such as Pinterest, Instagram...) or general audience social media that enable image sharing of this kind (Facebook, Tumblr, Twitter...) but also video sharing platforms that enable interested viewers to access a large number of protected works.

This marks a profound shift in paradigm compared to the application of hosting provider status hitherto invoked by the platforms<sup>52</sup> and unsuccessfully challenged in its principle by certain rightholders in the still image sector, as well as by rightholders in other sectors before that. Although they have often focused their legal actions on image referencing and display services (such as Google image search)<sup>53</sup>, many rightholders in the field of still images believe that sharing platforms engage in unauthorised acts of communication to the public of works belonging to their members. Such was the case when ADAGP came into conflict with Flickr (2007-2009): the court ruled that it had to provide the platform with a catalogue of the 25,000 works on which it claimed rights. The magnitude of the catalogues of protected works presents a major challenge: according to ADAGP, the 185,000 authors it represents hold a catalogue of close to 1 billion works. Thus, Article 17 will enter into force against the background of major expectations of interested parties.

As to which best efforts are likely to be conducted by platforms in the field of photography and visual arts, though, much remains to be built. It is true that the largest rightholders have, based on the catalogues of works for which they hold the rights, put together databases using fingerprinting technologies. This is the case, in France, of the ADAGP with its AIR (*Automated Image Recognition*) project: it includes a database of more than 500,000 works and is developed as part of an international project coordinated by CISAC (International Confederation of Societies of Authors and Composers). Without claiming to be exhaustive, the AIR database makes it possible to identify uses and claim rights on the works that raise the most substantial economic challenges. Likewise, the other collective management organisation in France for authors of still images, SAIF, created SAIF Images in 2015, a database that also holds some 500,000 works.

These various initiatives show that the huge scope of the catalogues of protected works in the field of photography and visual arts does not prevent protection on sharing platforms and that, quite to the contrary, certain rightholders have started to get organised in this spirit. It nonetheless remains that the “best practices” in guaranteeing the unavailability of works not authorised for sharing remain to be defined. It could well be that they will be based on fingerprinting systems to be implemented by the platforms, drawing on the information provided by the rightholders for each unauthorised work. However, these best efforts could also involve a different approach or a combination of other approaches out of all those described and analysed above in this report (watermarking, use of artificial intelligence to a certain extent research based on metadata,).

In any event, the definition of the best efforts in regard of unauthorised content will be decisive not only in guaranteeing the unavailability of certain works but also for the indirect effect it will undoubtedly have on the works whose sharing will be authorised. This is because, as is the case today

---

<sup>52</sup> Including when agreements were, by way of exception, signed by the sharing platforms with rightholders, for instance, YouTube and Dailymotion with ADAGP.

<sup>53</sup> See in particular the legal action initiated in vain by SAIF (Société des auteurs de l’image fixe) against Google which gave rise to a ruling by the Paris Court of Appeal of 26 January 2011 (copied here: [http://data.over-blog-kiwi.com/1/13/34/21/20140707/ob\\_0239d9\\_jugement-ca-paris-26-janvier-2011-goog.pdf](http://data.over-blog-kiwi.com/1/13/34/21/20140707/ob_0239d9_jugement-ca-paris-26-janvier-2011-goog.pdf)). Similarly, in 2016, Getty Images filed a lawsuit against Google over the Google Image service, but went on to withdraw it in 2018, under a licensing agreement that also reportedly included changes to certain linking practices.

in the area of music content, it is likely that the rightholders of the photography and visual arts sectors will overwhelmingly favour authorization of the sharing of their works over blocking and removal. The principle of authorisation laid down in Article 17 will enable the negotiations to get underway in this direction.

### 3.3.2. - Written works in the field of press and books.

Where the written word is concerned, the presence of protected works on sharing platforms is also a reality, which may be subject to the rules set out in Article 17.

This may be the case of platforms specialising in the written word (Scribd or Calameo or, in the field of scientific articles, ResearchGate) insofar as their main objective or one of their main objectives within the meaning of the Directive is indeed the sharing of protected works whose rights are held by third parties). In this regard, all the other sharing platforms and social media may be covered, insofar as they give access to written works.

Rightholders in the press and book publishing sectors are eligible to the legal regime set out by Article 17. Press content is shared massively. However, authors of press articles (and possibly their publishers who are assignees of these copyright where such assignment is applicable), are obviously authors protected by Article 3 of Directive 2001/29, and their rights fall within the scope of Article 17 as such.

As regards press publishers, although they are not mentioned in Article 3 of Directive 2001/29, to which Article 17 thus refers, it is nevertheless required, under the terms of Article 15 of Directive 2019/790, that they be granted “the rights provided for in Articles 2 and 3(2) of Directive 2001/29/EC for the online use of their press publications by information society service providers”. In other words, the neighbouring right recognised by Article 15 must enjoy the same protection as the copyright and neighbouring rights referred to in Article 3 of Directive 2001/29. A combined reading of Articles 15 and 17 of the Directive thus results in press publishers’ being regarded as also falling within the scope of Article 17 under the related right provided for by Article 15.

As a result of the protection attached to copyright and Article 15 neighbouring right, the sharing of press content on the platforms is therefore now subject to authorisation by the rightholders, who are entitled to expect the platforms to make their best efforts to prevent the sharing of unauthorised content. The definition of the best efforts likely to be carried out by the platforms cannot use, as reference point, the tools currently deployed on these platforms for the recognition of such content, since, according to the information gathered by the mission, the platforms do not deploy such tools. It remains to be determined, based on the overview of the content recognition tools described above in this report, what this obligation of best efforts actually entails.

In the book sector, the representatives of publishers met by the mission called attention to the presence on the platforms not only of audio books (the protection of which may presumably be ensured using the same technologies as those applicable to music content), but also of files corresponding to protected books or extracts (in pdf, epub or various image formats), in particular on closed user groups on social networks. They also mentioned , the practice of leafing through books,

which enables viewers to read them in effect by watching videos, and is said to be present particularly in the area of comics and manga<sup>54</sup>

The definition of the best efforts to be implemented by the platforms to block or remove written works used without authorisation, will depend on the application of the criteria set out in point 5 of Article 17<sup>55</sup>. As these platforms do not currently deploy recognition tools in this sector, there is no experience on their part on which to draw. As for rightholders, they do not seem to have yet explicitly set out a specific strategy on the issue of lawful sharing platforms, but rather tend to transpose to these platforms the tools that they develop to protect their rights across the whole digital world, including on massively infringing sites.

Rightholders in the field of written works will first, in the implementation of Article 17, need to identify the platforms on which the presence of works for which they hold the rights justifies an immediate full implementation of Article 17. This full implementation implies for them to provide the platforms with the relevant and necessary information which is necessary for them to carry out their best efforts in order to ensure the unavailability of unauthorised content.. In addition, the definition of the best efforts in guaranteeing the unavailability of unauthorised content requires a comparison of the available technologies and their effectiveness, including in light of the cost considerations and the principle of proportionality reiterated by the Directive.

### 3.3.3. - Rights of music authors, composers and publishers.

The rights of music authors, composers and publishers – like the related rights which producers also hold – are obviously subject to the authorisation regime made mandatory by Article 17 of the Directive. This authorisation regime will come in the wake of existing agreements between the main collecting societies and the main sharing platforms (with YouTube for SACEM for example since 2010, see 2.2.3.2.).

Even though these rightholders are very clearly aiming at a licensing regime, the scope of the best efforts to be made by the platforms is also of great importance to them. The best efforts music authors and expect from the platforms are likely to focus in practice, not only on the means to ensure the unavailability of unauthorised content but also on the accurate reporting of protected content used on the platforms.

At present, the recognition tools deployed by the platforms, based on fingerprints made of recordings as relevant, i.e., in light of the producers' neighbouring rights, only indirectly and partially reflect the

---

<sup>54</sup> even if this practice is perhaps not as massive as that of manga *scans*, probably engaged in primarily by sites whose main objective is to facilitate piracy, such that they do not fall within the scope of Article 17.

<sup>55</sup> By way of reminder, point 5 states that: “*In determining whether the service provider has complied with its obligations under paragraph 4, and in light of the principle of proportionality, the following elements, among others, shall be taken into account: (a) the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service; and (b) the availability of suitable and effective means and their cost for service providers.*”

exploitation of music authors' copyright in this case. This situation makes a complex reconciliation work necessary before rights can be effectively assigned to their authors (see 2.2.3.2.).

Through the notion of best efforts and the obligations of transparency, Article 17 should therefore enable greater traceability as far as authors', publishers', and musical composers' rights are concerned. The notion of best efforts may also cover technologies such as those that enable melody recognition, but also an improvement of information reporting based on the available metadata. As to the relevant and necessary information to be provided by the rightholders, it cannot consist of recordings or fingerprints made from the recordings, since these elements are not directly relevant to the works themselves, but they should consist of detailed information on the list of protected works.

### 3.3.4. - Audiovisual Authors' rights.

The rights assigned to audiovisual authors are obviously also affected by the authorisation regime provided for in Article 17. The concrete scope of the authorisation obligation will, however, depend on the identification of the relevant rightholders, and in particular on the debate as to whether it is transferred or presumed to be transferred to the audiovisual producer. Internationally, a variety of situations can be found. The Society of Audiovisual Authors (SAA), an association representing the collective management organisations of audiovisual authors at European level, also made a significant contribution to the European debate that led to the adoption of Article 18 of the Directive on the principle of appropriate and proportionate remuneration.

The implementation of Article 17, in its section on the issuance of authorisations, will raise the question as to whether existing experience in France of agreements between platforms (YouTube and Dailymotion, as it stands) and collective management organisations representing audiovisual authors (SACD and SCAM) should be extended. The answer will depend in part on the law applicable in each Member State as regards the assignment of rights to producers, and if necessary, on its combination with the principles laid down by Article 18 on the right to appropriate and proportionate remuneration for authors. In any event, authorisations will need to be issued by youtubers in their capacity as authors.

Where such authorisations are granted, the definition of the best efforts of the platforms raises issues comparable to those described above for songwriters and music publishers' authorisations. This is because collective management organisations do not seek to block or remove unauthorised content, but rather to license it. The key issue in defining the best efforts for them is therefore the reporting of information on acts of exploitation in order to be able to distribute the fees received. With this in mind, fingerprinting systems on video content provide a large part of the answer, in particular for authors of native audiovisual content on sharing platforms (e.g. youtubers). In addition, it would make sense for the issuance of authorisations by collective management organisations to at least result in increased reporting requirements.

### 3.3.5. – Music rights pertaining to “commercial use of music in graphic form”.

Similarly, rights pertaining to “commercial use of music in graphic form” (scores and song lyrics, the rights of which, as far as French publishers are concerned, have not been entrusted to SACEM but are individually managed by publishers), are likely to fall under the legal regime defined by Article 17. Many sharing platforms provide access to these works today, whether video or music file sharing platforms (particularly for song lyrics, including through “crowdsourced translation” or automated subtitles) or even specialised platforms fed by user contributions (for example lyrics.com or lyrics.net). Some of these platforms may operate on the basis of a license granted by music publishers for the exploitation of the works for which they hold rights (this is the case of paroles.net, a site that uses the BOEM database developed by the French Chambre syndicale des éditeurs de musique, following legal proceedings initiated by the Chambre syndicale). The general case, however, is that sharing platforms have neither a license agreement nor a recognition tool in place to identify and block unauthorised content.

In this area, Article 17 therefore opens up the possibility for rightholders to issue authorisations to platforms that should now clearly be regarded as carrying out acts of exploitation.

Defining the best efforts expected from platforms to block or remove unauthorised content requires a dialogue between the actors. In large part, the solutions around which discussion will centre are likely to be connected with the fingerprinting systems already applied to music recordings. In the case of protected lyrics appearing on the platforms as subtitles, the recognition of the audio fingerprint of the same title will be instrumental in detecting the use of the content. In other cases, the best efforts may include, if the use of the content by the platform warrants it and if the proportionality test is conclusive, the use of technologies based on character recognition. As for the relevant and necessary information to be provided by rightholders, it is expected to consist primarily of information on the list of repertoire protected, as is the case with songwriters and music publishers for other uses. Where a database of protected works exists, such as the BOEM database, it could also be put to use in connection with the best efforts conducted by the platforms.

In any event, as in other sectors, the solutions adopted for blocking and removing unauthorised content should logically also apply to monitoring authorised content exploitation.

### 3.3.6. - Rights of video game publishers.

Lastly, the legal regime defined by Article 17 of the Directive also applies in principle to rights held by video game publishers, assignees of authors’ rights or even certain related rights. Clearly, the content protected in this respect is widely shared on platforms falling within the scope of Article 17. Without even going into the debate on the ownership of rights on video game play (players versus game publishers), the cinematics and music produced for games are clearly massively protected subject matter on certain platforms.



However, the question of implementing Article 17 for this type of content remains to be answered, in a context where video game publishers, with the notable exception of the past practices of Nintendo<sup>56</sup> seem to favour the visibility that sharing platforms offer to their products over the collection of monetisation revenues.

### 3.4. - Content recognition tools will be central to the new balance between the parties interested in sharing protected content.

Aiming at a better protection of intellectual property rights, Article 17 amounts to a paradigm shift for online content-sharing service providers' practices and invites to a renewed approach of the balances of rights and interest hitherto prevalent. Although abundantly criticised by its opponents exclusively on the grounds of the constraints it will impose on acts of sharing, Article 17 nevertheless contains elements fostering balance between the prerogatives of rightholders, platforms and users. The definition of these new balances is not the least tricky of the challenges raised by its implementation.

#### 3.4.1. - For users: recognition tools, constraints and freedoms.

For the public using online content-sharing platforms, the rules laid down in Article 17 regarding the best efforts required to ensure the unavailability of unauthorised content have been widely presented by its most active opponents<sup>57</sup> as a factor that shrinks public liberties, allegedly sometimes even to the point of violating freedom of expression. "Upload filters" and the logic of upgrading protections on the various platforms for the different rightholders were thus central to the controversy surrounding the negotiation of Article 17.

As indicated above, this criticism fails to convince since it turns a blind eye to the current state of deployment of content recognition tools on online content-sharing service providers. It simply reasons as if the tools deployed by platforms without any control or obligation of transparency or were inherently preferable to the path followed by the European legislator, aiming at instituting appropriate balances and guarantees, and that is now time to implement in this spirit. .

##### 3.4.1.1. - *The balances and guarantees provided for by the Directive.*

Article 17 imposes in itself a logic of balances and guarantees, the fine-tuning of which constitutes one of the trickiest aspects of its implementation.

---

<sup>56</sup> From 2013 to 2018, Nintendo collected monetization revenue from YouTube videos using clips from its video games. The company had set up an affiliate program, called "Creators' Programme", which allowed users who uploaded the videos to donate some of the proceeds earned. The programme was halted at the end of 2018, when Nintendo decided to align with other major video game publishers and limit itself to requiring compliance with certain rules, for instance, requiring that the content include comments or creativity.

<sup>57</sup> In particular, the "Save your Internet" campaign: <https://saveyourinternet.eu/>

The first balancing factor resulting from Article 17 is the exemption from liability which its paragraph 2<sup>58</sup> implies for users in respect to sharing of protected content on platforms. It asserts the platforms' liability while also establishing an exemption from liability for the benefit of users *"when they are not acting on a commercial basis or where their activity does not generate significant revenues"*.

For users, paragraph 7 of Article 17 also provides that cooperation between platforms and rightholders with regard to blocking and removal as part of the best efforts of the platforms *"shall not result in the prevention of the availability of works or other subject matter uploaded by users, which do not infringe copyright and related rights, including where such works or other subject matter are covered by an exception or limitation"*. It lists the existing exceptions of which, in each Member State, users must be able to rely on *"when uploading and making available content generated by users on online content-sharing services: (a) quotation, criticism, review; (b) use for the purpose of caricature, parody or pastiche."* These exceptions, provided for on an optional basis by Directive 2001/29, are therefore binding on the Member States, at least as existing exceptions.

Paragraph 9 on the rapid and effective complaints and redress mechanism provides the framework for ensuring the application of these exceptions. It offers users new guarantees in managing conflicts in the event that content is blocked or removed. It states that the rightholders' requests for blocking and removal must be duly substantiated. It adds that complaints should be dealt with without undue delay and removal decisions should be verified by a natural person. It also provides that out-of-court redress mechanisms must be available for the settlement of disputes, in such a way that these may be settled impartially, without depriving users of the legal protection offered by national law and without prejudice to their right to use effective judicial remedies, in particular to assert the benefit of an exception or limitation.

Still in this paragraph 9 on the system for handling complaints and appeals, Article 17 stresses that: *"This Directive shall in no way affect legitimate uses, such as uses under exceptions or limitations provided for in Union law, and shall not lead to any identification of individual users nor to the processing of personal data, except in accordance with Directive 2002/58/EC and Regulation (EU) 2016/679"*. It provides for information to users by the platforms on the possibility of using works and other protected subject matter within the framework of exceptions or limitations to copyright and related rights provided for by Union law.

Lastly, paragraph 10, which deals in particular with dialogue between interested parties, provides for the participation of organisations representing users and other stakeholders. It stresses that *"When discussing best practices, special account shall be taken, among other things, of the need to balance fundamental rights and of the use of exceptions and limitations"*.

---

<sup>58</sup>"Member States shall provide that, where an online content-sharing service provider obtains an authorisation, for instance by concluding a licensing agreement, that authorisation shall also cover acts carried out by users of the services falling within the scope of Article 3 of Directive 2001/29/EC when they are not acting on a commercial basis or where their activity does not generate significant revenues."

### 3.4.1.2. - The issue of legitimate uses, and in particular maintaining the benefit of exceptions.

All the provisions described above attest to the balances sought by the European legislator and the importance it has placed on giving users the chance to continue to benefit from the legitimate use of works and other protected subject matter, despite the removals and blockages. This concern relates, for example, to the use of protected works and subject-matter in the public domain, which, in the absence of protection by copyright or related rights, should not be subject to removal or blocking. It also covers the use of works authorised by a licence, the rights of users falling in step here with those of the rightholders who issued the licence connected with the use of their content.

The debate focused above all on protecting the benefit of exceptions for users, even to the point of triggering scaremongering campaigns about the so-called ban on *memes*<sup>59</sup> and *gifs*<sup>60</sup> if the Directive was adopted.

The legal assessment called for by the application of exceptions necessarily raises tricky questions, in particular at a time when digital tools put reuse within easy reach of any user<sup>61</sup>. They are frequently invoked, even in good faith, in cases where it is not certain that they are applicable<sup>62</sup>. In the context of online content-sharing service providers, this applies in particular to parody, pastiche and caricature and to “short quotations” (“analysis and short quotations substantiated by the critical, polemical, pedagogical, scientific or informational nature of the work to which they are incorporated” in French legislation<sup>63</sup>), whereas the Directive pays particular attention to this ability for users to invoke the benefit of existing exceptions.

Analysed in the light of the experience of the recognition tools already deployed on certain online content-sharing platforms, the debate might be minimized if a purely quantitative approach was taken. It emerges from the interviews conducted by the mission that, very often, the removals operated *via* content recognition tools are not contested and that, when they are, the reasons invoked rarely seem

---

<sup>59</sup> A meme is defined as a concept (text, image, video) that is massively reproduced, varied and re-appropriated on the Internet in an often parodic manner, and spreads like a virus. It can be created from an element protected by copyright or a related right.

<sup>60</sup> A *gif* (for *graphic interchange format*, or image exchange format) is a digital image format commonly used on the web, by which short animations can be reproduced. It can be created from one or more elements protected by copyright or a related right.

<sup>61</sup> See the report of the CSPLA mission on transformative works placed under the responsibility of Ms Valérie Laure Benabou, rapporteur Mr Fabrice Langrognet: <https://www.culture.gouv.fr/Sites-thematiques/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-propriete-litteraire-et-artistique/Travaux/Missions/Mission-du-CSPLA-relative-aux-creations-transformatives>

<sup>62</sup> On the interpretation of the scope of the producer’s exclusive right to the quotation exception in the case of sound sample snatches (*sampling of music*), see the recent ruling C-476/17 Pelham of 29 July 2019, which states that “that the reproduction by a user of a sound sample, even if very short, of a phonogram must, in principle, be regarded as a reproduction ‘in part’ of that phonogram, unless the sound sample is used in a modified form unrecognisable to the ear”, and that the notion of quotation implies that the person invoking it aims to enter into dialogue (illustrating an assertion, defending an opinion, “intellectual comparison”) with the work from which the sound sample is taken, but “does not extend to a situation in which it is not possible to identify the work concerned by the quotation in question”.

<sup>63</sup> Article L. 122-5 of the French Intellectual Property Code.

to fall under one of the exceptions provided for by the legislator. A large proportion of the counter-notifications seems not to be really substantiated with regard to the exceptions provided for by the legislator (Article L. 122-5 of the French Intellectual Property Code) and applied by the judges. YouTube points out that, in the case of blockings and removals carried out on the basis of “manual” rightholders’ claims, two-thirds of counter-notifications from users disputing blockings or removals are rejected by its own teams (and not even forwarded to the rightholders) for lack of solid grounds (see 2.1.1.2.).

The issue of exceptions is nonetheless a real and important one in principle. As stated above, the actual benefit from exception is one of users’ top expectations, especially some youtubers. This legitimate request must be heard.

Content recognition tools raise a real question as to how the benefit from exceptions can be maintained. By nature, these technical tools cannot carry out the detailed assessment needed to decide on the benefit of exceptions, which requires complex legal appreciations and ultimately depends on the appreciation of the judges. This is the case with regard to short-quotation exceptions, which French legislation and case law, including that of the Court of Justice of the European Union, make dependent on an assessment that is not purely quantitative. The same applies to the exceptions of caricature, pastiche and parody, or to case law applying the theory of accessory or accidental inclusion, which obviously involve precise and complex assessments.

The sensitivity of this subject in the context of the negotiation of Article 17 was fuelled by the way such disputes are handled when a content is blocked on YouTube, within a bilateral dialogue between the user and the rightholder. This system, set up by YouTube with the stated objective of avoiding arbitrating on complex cases, is sometimes criticised by users, who call for an impartial dispute settlement body to be established.

Lastly, the dynamic of constant technological progress is fanning fears that the expanses of freedom preserved by technologies’ limitations will ultimately disappear: concretely, whereas fingerprint recognition technologies, at the time of their initial deployment, needed excerpts of at least 15 or 20 seconds in duration to yield conclusive results, they can now trigger blocking based on excerpts as short as 5 seconds and sometimes even much less. Thus, as technology improves, it is sharing practices that are likely to become increasingly hampered.

While all these factors explain the sensitivity to the topic of exceptions, they neither invalidate the approach underpinning Article 17, nor the use of content recognition tools. Quite to the contrary, they fully justify the search for balance and guarantees characterising the work of the European legislator, and ultimately the very principle of its action.

### *3.4.1.3. - Consequences to draw on the complaints and redress mechanism.*

The Directive sets out in paragraph 9 a complaint and redress mechanism that should guarantee that the benefit of the existing exceptions made compulsory by paragraph 7 is maintained.

The reference to exceptions in paragraph 9 of Article 17 relating to these arrangements is significant in this respect. Similarly, it should be noted that recital 70 introduces a strong link between the

exceptions and limitations made compulsory and their implementation within the framework of the complaints and redress system: *“Those exceptions and limitations should, therefore, be made mandatory in order to ensure that users receive uniform protection across the Union. It is important to ensure that online content-sharing service providers operate an effective complaint and redress mechanism to support use for such specific purposes”*.

This complaint and redress mechanism is designed to provide effective responses to the difficulties revealed by experience with existing recognition tools in several ways. The Directive requires speed and efficiency. The removal or blocking request made by the rightholder must be duly substantiated. The request must be processed *“without undue delay”*. Decisions to block or withdraw *“are overseen by a natural person”*.

Above all, paragraph 9 of Article 17 introduces the obligation to provide for *“out-of-court redress mechanisms”* for the settlement of disputes. These mechanisms must enable *“impartial dispute resolution”*. It is specified that they do not deprive the user of the legal protection granted by national law, as users must be able to turn to a court or other competent judicial authority to assert the benefit of an exception or limitation to copyright and related rights.

With these requirements, Article 17 therefore draws on the experience with existing recognition tools and responds to one of the main criticisms of users, particularly youtubers, regarding the dispute settlement procedure, which they saw as ultimately left to the discretion of rightholders. It therefore marks a real step forward in guaranteeing the benefit of exceptions.

At the transposition stage, it is important that this balance be put into practice. For instance, under the draft legislation on the audiovisual policy in the digital era, currently under consideration by the French Parliament, it is envisaged to entrust the future Authority for the regulation of audiovisual and digital communications (ARCOM) with competence in this matter. The Authority must be able to fully play the part provided for by Article 17 in the impartial settlement of disputes.

Similarly, in the case of an unwarranted request for removal or blocking, for which it would be established that the filing party was aware that it was unfounded, sanctions could conceivably be provided for, as already provided for, on a quite similar topic, by paragraph 4 of Article 6 of the law for confidence in the digital economy<sup>64</sup>. While such a provision is likely to be applied only in rare of cases, it does mark the balance in the rights and duties of the parties in implementing removals and blockages.

---

<sup>64</sup> “4. Any person depicting content or activity to the persons mentioned in paragraph 2 as being unlawful in order to obtain its removal or to stop its dissemination, with the knowledge that this is inaccurate information, shall be subject to a penalty of one year’s imprisonment and a fine of €15,000.”

#### *3.4.1.4. – A point to consider on content management rules.*

In addition to an effective complaint and redress mechanism, the balance sought by the European legislator also calls for careful analysis of the impact of the management rules adopted by rightholders when it comes to content recognition, blocking and removal.

Within the framework of existing recognition tools, precise content management rules are defined by the rightholders, in particular on some platforms. They may include duration thresholds from which the rules they define (blocking, monetisation or manual verification) are applied, as well as thresholds calculated in proportion to the content recognised in the video examined. These rules play a decisive part in the definition of the sharing options opened to users: depending on whether, for a given content item, the blocking threshold is set at 15 seconds or 5 minutes, the user will have a completely different sense of the constraint resulting from the application of the content recognition system.

The management rules are entirely the rightholders' prerogatives. By subjecting to their authorisation the act of communication to the public by platforms, Article 17 implies that rightholders have the possibility not to authorise the presence of works and other protected subject-matter on the online content-sharing platforms and to determine the precise limits of such presence. It is important that this prerogative be preserved. The specificities of each sector and the choices of each rightholder must be duly taken into account.

This freedom of the rightholder in the definition of content management rules must go hand in hand with a full analysis of their exact impact. It is important that the management rules applied make it possible to take the best possible account of the balance established by Article 17 regarding the sharing of works and other protected subject matter.

Whereas the performance of technical recognition tools makes it possible to block the sharing of extremely short excerpts<sup>65</sup>, the balance sought by the legislator may not be fully achieved if all the faculties offered by the development of technologies were to consistently result in blocking and removal. In negotiating Article 17, the European Commission suggested as much, when it denied the allegations that the Directive would prohibit memes and gifs<sup>66</sup>.

A voluntarily effort of interested parties to address this concern would make it possible to fully reflect the search for balance reflected by the Directive, facilitating its implementation without harming the legitimate interests of rightholders. Given the practices currently observed on online content-sharing platforms, where blocking rules do not apply to excerpts lasting less than a few seconds, this discussion, which should fully take into account the diversity of sectors and content, should be possible. Envisioned as voluntary best practices, possibly concerted and shared rather than in the context of a legal debate on the scope of exceptions, which is of another nature, this approach would facilitate effective and pacified implementation of the Directive.

---

<sup>65</sup> One operator interviewed by the mission mentioned the possibility of protected content recognition from an excerpt as short as 0.5 seconds.

<sup>66</sup> <https://ec.europa.eu/digital-single-market/en/faq/frequently-asked-questions-copyright-reform>

The discussion on this voluntary approach could in particular be opened in the framework of the dialogue between stakeholders conducted by the European Commission for the purpose of the Commission's publication of its guidance on the application of article 17. Paragraph 10 of article 17 provides that "*When discussing best practices, special account shall be taken, among other things, of the need to balance fundamental rights and of the use of exceptions and limitations*". Another aspect of this discussion of best practices = could also cover the suitable level of publicity as far as management rules for unauthorised content are concerned.

### 3.4.2. - The case of professional or semi-professional users: towards an increasingly organised dialogue with the rightholders of shared content.

Article 17 of the Directive makes a distinction between users of online content-sharing platforms according to whether they are acting in a non-commercial capacity or in another capacity. Paragraph 2 provides that authorisations issued to platforms only cover actions performed by users "*when they are not acting on a commercial basis or where their activity does not generate significant revenues*", in other words when they are individuals (or non-profit entities) who do not derive significant revenues from the activity in question.

It can be deduced from this that the authorisation which rightholders can provide to platforms pursuant to Article 17 of the Directive does not cover acts of sharing that are carried out by "institutional" or "official" accounts and channels that can be created and operated by content producers, advertisers, brands or even media. It also does not cover youtubers (or videographers) who derive significant revenue from their YouTube channel, or even accounts on other social media maintained by "influencers", as long as their activity on these networks can be viewed as generating significant revenue.

In both of the above cases, "official" accounts or accounts managed by youtubers and influencers generating significant revenue, Article 17 does not further specify the legal regime applicable to the issuance of authorisation. However, it can be assumed that the platform carries out an act of commercial use when it gives the public access to any protected content, regardless of the commercial or non-commercial context in which the user shares the content. An authorisation must therefore be issued in all cases. Thus, for the platform not to incur its liability in this respect, either an authorisation issued directly to "commercial" users by rightholders should be delivered or a legal mechanism should be negotiated between rightholders and the platform to extend the benefit of the authorisation issued by the platform to "commercial" users. Such an additional authorisation would fall within the scope of contractual negotiation between rightholders and platforms. It is difficult to see *a priori* what would be contrary to its principle in the Directive.

Whether this involves a separate negotiation or a negotiated extension of the authorisation issued to the platforms, rightholders will therefore determine the terms and possibly the limits that they intend to place on the sharing of their works and other subject matter protected by these "commercial" users.

The situation will not necessarily be the same with all types of uses on the various platforms. Above all, it will probably not be the same for brands that publish on social media, for the accounts of television channels and other broadcasters, for the official accounts of music or film producers or for the accounts of video producers and influencers.

It is possible that in certain cases, the “commercial” user will overwhelmingly post content on which he/she holds rights. This will be the case, for example, with the official channels of music producers, on which they post their own recordings and clips. The same can apply to accounts held by brands for the purpose of publishing promotional content: these may include a measured quantity of content on which users can ensure that they hold rights through licensing agreements. In these scenarios, the authorisation to share and the related management methods should not pose any major difficulties.

As for videographers and influencers, their activity can entail extensive sharing of content owned by third parties. In addition, they are by nature more numerous and less well positioned to enter negotiations with rightholders with a view to securing authorisations from them directly. Although they are excluded from the scope of the authorisation issued to platforms pursuant to Article 17, if their activity generates significant revenue, they are therefore in a situation, in many respects, comparable to that of non-commercial users. It is with regard to them that an extension of the authorisation issued to the platforms by the rightholders would be most justified.

Regarding the best efforts of the platforms to ensure the unavailability of unauthorised content, Article 17 applies in the same way to all user accounts, whether they act on a commercial or non-commercial basis. As a result, the logic of the best efforts of the platforms and the obligation on rightholders to provide relevant and necessary information for this purpose also applies indiscriminately to the accounts of “commercial” users, including those of youtubers and influencers.

Article 17 also requires that all forms of sharing that do not infringe copyright or a related right, including where they fall within an exception or limitation, must be guaranteed for such “commercial” users, as well as for non-commercial users.

For these users, any unjustified blocking or removal decision may jeopardise the very sustainability of their activity. The measures that must be taken in accordance with the Directive to ensure that the benefits of exceptions are maintained are therefore of particular interest to them : obligation on rightholders to duly justify their blocking or removal request, obligation to take a decision without undue delay and on the basis of a review carried out by a natural person, and not a purely automated process, establishment of a complaint and redress mechanism and impartial dispute settlement. They are also particularly interested in the discussions that could be initiated regarding the content of the management rules set by the rightholders and possibly their degree of publicity.



3.4.3. - Between rightholders of shared works: Article 17 will lead to greater formalisation of the rules applicable in the event of conflicts of rights or rules.

The implementation of Article 17 is expected to also lead to a formalisation of practices and rules where the sharing of content gives rise to competing claims by several rightholders.

It is relatively common for the use of an online content-sharing platform to trigger competing claims. The same applies to video-sharing platforms, in the case of videos that contain excerpts of several contents that have given rise to fingerprints, which may be musical or film excerpts.

The identification of a single protected content could also lead to a conflict between rightholders. While fingerprinting systems are designed to allow only one fingerprint to be made per protected content (known as an "asset"), the fact remains that the territorial application of rights can lead to competing claims within the same territory (particularly if "world" rights have been mistakenly associated with the fingerprint).

The rule applied by YouTube in the event of competing claims consists of applying the most restrictive rule (blocking if one of the rightholders has chosen monetisation and another chose blocking). The platform invites the rightholders to reach a direct agreement. Through its interface, the platform allows for dialogue between rightholders. It gives them a timeframe within which they must reach an agreement. The sums generated by the video are put in reserve.

As for the *Rights Manager* tool implemented by Facebook, it provides, when multiple claims by rightholders result in monetisation requests, that the income from the video in question is shared equally between them (regardless of the respective duration of the protected excerpts used). In the event of a conflict, the sums are also placed in reserve.

In the context of the implementation of Article 17, a clear framework will need to be defined to address potential conflicts between the rules set or claims filed by rightholders.

Article 17 thus requires that the measures taken by a platform proceeding from its best efforts do not infringe on the exploitation of a work that is the subject of a license, and of which the user, as well as the rightholder who issued the license, can legitimately expect that it can be shared<sup>67</sup>.

As regards the complaint and redress mechanism provided for in paragraph 9 of Article 17, and the intervention of an out-of-court redress mechanism enabling an impartial settlement of disputes, they do not appear to be applicable to disputes between rightholders. Paragraph 9 provides that the complaint and redress mechanism is "*available to users*".

---

<sup>67</sup> Recital 66 already referred to above specifies that: "*The steps taken by online content-sharing service providers in cooperation with rightholders should not lead to the prevention of the availability of non-infringing content, including works or other protected subject matter the use of which is covered by a licensing agreement, or an exception or limitation to copyright and related rights*".

### 3.4.4. - The definition of these new balances requires a dialogue and shared guidelines, with a major role for the European Commission.

In view of the change in paradigm operated by Article 17 and the complex issues which its implementation raises, the method chosen by the public authorities for the transition into the new legal environment takes on crucial importance.

In Article 17, this point is addressed by paragraph 10 on the dialogue between interested parties and the guidance which the European Commission is expected to address on the Article's application, in particular paragraph 4 (on best efforts): *“As of 6 June 2019 the Commission, in cooperation with the Member States, shall organise stakeholder dialogues to discuss best practices for cooperation between online content-sharing service providers and rightholders. The Commission shall, in consultation with online content-sharing service providers, rightholders, users' organisations and other relevant stakeholders, and taking into account the results of the stakeholder dialogues, issue guidance on the application of this Article, in particular regarding the cooperation referred to in paragraph 4. When discussing best practices, special account shall be taken, among other things, of the need to balance fundamental rights and of the use of exceptions and limitations. For the purpose of the stakeholder dialogues, users' organisations shall have access to adequate information from online content-sharing service providers on the functioning of their practices with regard to paragraph 4.”*

The continuation of dialogue at European level and the definition of guidelines by the European Commission are essential for the proper functioning of the single digital market and in order to avoid any risk of circumvention of the requirements laid down by the Directive.

According to the Berne Convention and the so-called Rome II regulation on the law applicable to non-contractual obligations<sup>68</sup>, in principle, for rules concerning protection against infringements of intellectual property rights, the law of the country where protection is sought applies. This rule on applicable law should enable each Member State, in contrast to the country of origin principle set out in particular by the Electronic Commerce Directive, to define protective rules in the implementation of Article 17.

However, considering both the aim to fully attain the objectives set out and the issues at stake in ensuring the consistency of the single market, a high level of protection should be sought for the whole of the European Union. In applying the Directive, a number of essential concepts built into Article 17, including the notion of best efforts or that of relevant and necessary information, would gain from having a uniform interpretation. Under these conditions, the dialogue to be conducted and the guidance to be issued by the European Commission will be of essential importance in the implementation of article 17.

This dialogue at the European level should pertain in particular to:

---

<sup>68</sup> Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II).

- The identification of the platforms concerned by article 17 and the method for defining the thresholds that it provides, in particular with regard to the *“significant quantity of works protected by copyright or other protected subject matter”*;
- The situation of the various rightholders entitled to grant authorisations provided for in Article 17 for each type of platform, depending on the type of content found on these platforms;
- The definition of the best efforts notions set out in paragraph 4 of Article 17, as paragraph 5 provides that it must take into account *“(a) the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service; and (b) the availability of suitable and effective means and their cost for service providers”*.
- The definition of *“relevant and necessary information”* that must be provided by rightholders to platforms so that they can deploy these *“best efforts”* under Article 17.4.b. Depending on the sectors and rightholders, these informations may consist of files corresponding to the protected works or subject matter (or works databases) or elements enabling its protection (digital fingerprints) but also, in particular in cases where the rightholder does not have the copy of the work required for recognition, information on the list of protected works;

On these last two points, the respective situations of various different sectors (music, audiovisual, photography, books, press, video games, etc.) will need to be given special attention and will justify the fact that the interested parties conduct an in-depth dialogue with each other, which should not be barred by competition law considerations ;

- The definition and periodicity of *“adequate information on the functioning of their practices”* to be provided by platforms in accordance with paragraph 8 to rightholders *“with regard to the cooperation referred to in paragraph 4 and, where licensing agreements are concluded between service providers and rightholders, information on the use of content covered by the agreements”* as well as adequate information mentioned in paragraph 8 to be accessed, for the purpose of dialogues with interested parties, by user organisations.

Beyond the dialogue between the parties already initiated by the European Commission and the guidelines that it will define on this basis on some of these issues, Article 17 requires long-term dialogue.

The implementation of Article 17 will require a dynamic assessment of its requirements, taking into account both changes in content sharing practices and changes in the technologies available to guarantee the unavailability of content.

In the draft law on the audiovisual sector in the digital age, the French Government plans to entrust the competent regulatory body with an assessment and expertise mission that is expected to play an important part in bringing objectivity to the debates and ensuring the rules are duly implemented. This issue could also be addressed within the framework of a long-term dialogue between the parties at European level.



## Conclusion

In concluding this survey of a subject that is as important for the future of digital content uses and the effectiveness of creators' rights as it is complex and still little known, three conclusions are in order.

First, as extensive as the presentation in this report is, buttressed by multiple hearings, in-depth technical testing and quantitative and qualitative opinion polls, it is only one step along the way towards better shared knowledge of the recognition tools currently deployed on content-sharing platforms. This effort must continue. Recognition tools are a decisive parameter in the operation of these platforms, which are themselves now major players in the expression of the public, the dissemination of knowledge and the distribution of creative works. The information asymmetries that characterise these tools make it all too easy, depending on each person's interests or *preconceptions*, to caricature them as dangerous weapons of censorship or as miracle solutions for protecting rights. The technological complexity, confidentiality issues of the contractual agreements and the power of the economic players involved must be overcome to allow progress towards a better understanding of the issues at stake, and ultimately a better deployment of the recognition tools.

Secondly, appropriate governance for the change called for by Article 17 remains to be defined and implemented. The Directive provides for stakeholder dialogue and the definition of guidance by the European Commission. This process is already underway, with several meetings held or scheduled. It is complex but essential. The concertation between the players, within each of the creative sectors, but also between platforms rightholders and users is essential. A European approach is needed to work out the right balances. It will make it possible to integrate the contributions and role of national regulators, which will also be decisive, including over time, in particular to ensure a realistic and dynamic assessment of the concepts of "best efforts" of platforms and of "relevant and necessary information" to be provided by rightholders.

Lastly, the paradigm shift enshrined in Article 17 is both a matter of principle, with the affirmation of copyright application, and of modalities, with the role played by the cooperation of interest parties.. Article 17 could – and should! - go almost unnoticed by the vast majority of users. For platforms and rightholders, the story is very different. The basic idea underlying Article 17, consisting of effectively applying copyright to online sharing services, is hardly disputable, given the way in which platforms operate and the magnitude of their use – hence its successful adoption, despite the conflicting interests and controversies raised. At the same time, as far as modalities are concerned Article 17 launches a promising process, the ambition of which does not rule out some pragmatism, based on a

logic of conformity, or *compliance*<sup>69</sup>, very familiar to other sectors<sup>70</sup>. The objectives chosen, in this case the effectivity of rights alongside easy digital content use, are being implemented by the players in a logic different from that of traditional legislation or regulation. Once the principles have been established, the key will be to determine the governance mode, shared rules, monitoring thereof and integration of all the aforementioned in the operation of the recognition tools.

By adopting Article 17, the European Union has, as it did previously on another subject when it adopted the General Data Protection Regulation (GDPR), sent a strong message to international players: copyright is not a survivor of yesterday's world but indeed an integral part of the model of digital uses to which Europe is committed -- a model which it has found the appropriate means to enforce.

---

<sup>69</sup> On this subject, see the report by Marie-Anne Frison-Roche, *The contribution of compliance law to Internet governance*, submitted to the French Secretary of State for Digital Affairs (July 2019), who hailed the adoption of Article 17, described as a mechanism for compliance law. See [https://www.economie.gouv.fr/files/files/2019/Rapport\\_MAFR\\_Compliance\\_et\\_Gouvernance\\_du\\_numerique\\_juin\\_2019.pdf](https://www.economie.gouv.fr/files/files/2019/Rapport_MAFR_Compliance_et_Gouvernance_du_numerique_juin_2019.pdf).

<sup>70</sup> Examples include company internal governance measures (Sarbanes-Oxley Act, in the United States, 2002), personal data protection (company correspondents) and competition law (tracking of action on commitments).

# Appendices

## 1 - Mission letter



Paris, le 29 MARS 2019

Monsieur Jean-Philippe Mochon  
Conseiller d'Etat



Conseil supérieur  
de la propriété  
littéraire et artistique

Le Président

182, rue Saint-Honoré  
75033 Paris Cedex 01  
France

Téléphone : 01 40 15 38 73  
Télécopie : 01 40 15 88 45  
cspla@culture.gouv.fr

<http://www.culturecommunication.gouv.fr/Thematiques/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-proprietee-litteraire-et-artistique>

Monsieur le Conseiller,

Les outils de reconnaissance des œuvres sur les plateformes numériques de partage de contenus constituent aujourd'hui un aspect crucial tant du respect du droit d'auteur et des droits voisins que, à travers les accords avec les ayants droit dont ils permettent la mise en place, de la rémunération de la création. L'article 17 de la nouvelle directive européenne sur le droit d'auteur dans le marché numérique leur donne une portée renforcée, en transformant ces outils, mis en place de manière volontaire, en dispositifs appelés par le droit de l'Union européenne et encadrés par lui.

Le rapport sur ce sujet de la mission d'étude du CSPLA dont j'avais la responsabilité, présenté en décembre 2017, a permis de dresser un premier état des lieux des outils existants, des bonnes pratiques et de leurs limites. Montrant tant la réelle utilité des outils de reconnaissance automatique des contenus que les limites d'une approche fondée uniquement sur le volontariat, il a fortement encouragé l'adoption de l'article 17 de la directive sur le droit d'auteur, tout en suggérant des pistes d'amélioration. Certaines de celles-ci, portées par les négociateurs français et les parlementaires européens, ont été reprises dans le texte adopté par le législateur européen.

Dans le prolongement de ce rapport, je souhaite vous confier une mission pour approfondir l'analyse de l'efficacité de ces outils techniques, identifier les points sensibles que soulève leur mise en œuvre et formuler des propositions dans la perspective en particulier de l'évolution du cadre juridique européen.

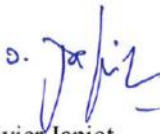
Pour la première fois, cette mission du CSPLA prendra la forme d'une étude conjointe avec deux autres institutions, l'HADOPI et le CNC, que tant leurs missions légales que leur expertise qualifient tout particulièrement pour un tel exercice. Bénéficiant de l'acquis de réflexion de chacune des trois institutions, ainsi que de leurs ressources, l'étude conjointe devrait représenter une contribution importante à la définition d'une doctrine française et européenne sur un sujet essentiel.

Afin de mener à bien cette mission, vous procéderez à des auditions des membres du CSPLA qui le souhaitent ainsi que des entités et personnalités dont, avec le CNC et l'HADOPI, vous jugerez utiles les contributions, y compris à l'échelle européenne ou internationale. Vous serez assisté par M. Sylvain Humbert, maître des requêtes au Conseil d'Etat, qui a accepté d'être le rapporteur de la mission.

Il serait très souhaitable que la mission puisse faire l'objet d'une première présentation détaillée au CSPLA avant l'été avant de rendre ses conclusions d'ici l'automne prochain.

Je vous remercie d'avoir accepté cette mission et vous prie de croire, Monsieur le Conseiller, à l'expression de mes sentiments distingués.

*Avec plaisir,*

  
Olivier Japiot



## 2. - Characteristics of content recognition tools

The interviews carried out by the mission helped bring to light a range of characteristics, varying in importance, of content recognition solutions, including the criteria available for the creation of content management rules by right holders, possible actions and functionalities offered by the various tools.

Some of these aspects, generally the most fundamental, are already taken into account by the majority of existing solutions. Others, however, all the while addressing certain expectations and problems, are implemented by few, if any, content recognition solutions.

This appendix therefore endeavours to recapitulate the list, not exhaustive at this stage, of the points raised during our meetings with rightholders, content sharing platforms and platform users.

### **Criteria for rule management**

<b>Criteria available for a majority of solutions</b>	<b>The rule applies...</b>
Duration	...depending on a minimum (or maximum) duration of the excerpt used.
Percentage of original content	...if the excerpt used is greater (or less) than a certain percentage of the original content.
Percentage of content shared by the user	...if the excerpt used is greater (or less) than a certain percentage of the content shared by the user.
Audio / video (for audiovisual content)	...if the excerpt used matches the audio and/or video of the original content.
Place	...if the shared content is viewed from one or more specified territories.
White List	...unless the uploader is on a predefined white list.
Level of confidentiality	...if the content uploaded online is public, unlisted, restricted or private.
Sharing mode (if applicable)	...if the content is uploaded on a personal profile or on a community page.

<b>Criteria not offered or available on only a few solutions</b>	<b>The rule applies...</b>
Date	...until (or from) a given date.
Level of certainty	...if the excerpt used has a level of resemblance higher (or lower) than a certain threshold.
Continuous / disjointed	...depending on whether the match detected is a continuous excerpt of the original content or an aggregation of small excerpts.
Segment	...if the excerpt used comes (or does not come) from a specific segment of the original content.
Type of device	...if the content uploaded online is viewed from a computer, tablet, smartphone, connected box, etc.
Age restriction	...if the content uploaded by the user is subject (or not) to age restrictions.

### **Possible actions for rightholders on content posted online by users**

<b>Actions available on a majority of solutions</b>
Blocking content
Claiming all advertising revenue
Monitoring
Manually approving

<b>Actions not available or available only on a small range of solutions</b>
Prohibiting monetization (content can be shared but not monetised through advertising)
Requiring monetization (content can only be read if advertising can be displayed)
Sharing revenue (e.g. with the user who uploaded the content)
Replacing the copied content with the original version (of better quality)
Adding a link or reference to the content shared by the user (e.g. link to an official site)
Sending an alert to a recipient or a third-party system (e.g. digital tattoo analysis system)

### **Practical features offered by content recognition solutions**

<b>Features available on most solutions</b>
External digital fingerprint generation
Back-compatibility of former fingerprinting tools
Exclusion of certain parts of content in the fingerprint
Management of territoriality of rights on content
Optional mass and automated insertion of content into the reference database
Management of multiple matches between analysed content and multiple protected content
Interface for resolving conflicts between fingerprints
Interface for resolving disputes filed by users
Retroactive analysis of content posted before fingerprint generation
Granularity of rules (by rightholder, content group, channel, content, etc.)
Immediate consideration for new fingerprints

<b>Practical features not available or available only on a few solutions</b>
Programmed management of commercial use windows on content
Management of a list of content that cannot be monetised or blocked (public domain, copyright-free content)
Function to test, before posting, whether content is likely to be claimed by one or several rightholders
Deletion of passage targeted by a claim within content shared by a user
Substitution of the passage targeted by a claim within content shared by a user
Ability to share advertising revenue in proportion to identified usage
Detailed activity report publishing, about matches and claims made by the system, for rightholders (ideally, based on a standardised format)
Recognition of identical content, through hashcode comparison, in order to identify content that has possibly already given rise to a claim
Content recognition by watermark analysis
Fingerprint generation from content shared by a third party and subject to a manual claim made by the rightholder

Prioritisation of claims and disputes handling based on contextual data, thanks to intelligent sorting algorithms (smart filtering)
Detailed and practical information about changes and improvements implemented into a content recognition technology during an upgrade (system update, new generation of fingerprints, etc.)
Transparent alert procedure for rightsholders in case of dysfunction or failure (even if just temporary) of a recognition tool

### 3. - Further details on technology robustness assessments

The assessment protocols developed by the scientific community are now able to test the effectiveness of content recognition technologies in a relatively exhaustive manner, using proven methods.

However, in practice, upon assessing audio or video content recognition technologies, it becomes clear that professionals in the music or audiovisual industry have generally developed their own test protocols, based primarily on the analysis criteria which they consider to be most relevant. To wit, many technologies have been tested since the late 2000s by rightholders and their representatives, following a fairly well-defined method that consists of submitting several hundred or even several thousand actual cases to the recognition tools in order to determine how far the recognition technologies work. These methods are defined by experts, generally working for rightholders. In most cases, they remain confidential, as do the resulting findings.

Given the time and resources available within the framework of this mission, and the evaluation works previously carried out at the initiative of many rightholders and their representatives, the decision was made to carry out targeted tests.

The aim was to carry out a series of stress tests, based on a set of tests consisting of representative scenarios.

The cases tested are grouped by level of difficulty, from basic posting of excerpts of protected content online to more or less tightly-restricted combinations of effects. The types of alterations tested reflect both observed user practices and cases reported by rightholders during the hearings conducted by the mission.

Below is a summary of the effects tested (on several different types of audiovisual content):

<b>Test Set 1 (excerpts)</b>
3 Minute excerpt
7 Minute excerpt
15 Minute excerpt

<b>Test Set 2 (moderate alterations)</b>
Video acceleration (+15%)
Video acceleration (+30%)
Side-by-side display of two distinct content items
Addition of random noise to video (50%)
Application of an "old film" effect
Application of a moderate continuous distortion effect
Deterioration of video quality
"Camcording" effect (change of perspective)
Vignetting effect
Montages using excerpts of varying durations
Montages using excerpts of differing content

Video slowdown (-15%)
Video slowdown (-30%)
Three-fold replication in image of original video
Image rotation 10°
Image rotation 180°
Image rotation 90° to the left
Logo overlay on image (25% of surface)
Opaque mesh overlay covering 50%
Zoom (+10%) and image offset upward and to the left
Zoom (+20%)
Zoom (+25%) and image offset upward and to the left

<b>Test Set 3 (significant alterations)</b>
Video acceleration (+100%) and change in tone
Alternating zoom (+10%) and normal speed + colour and B&W video
Application of moderate "shaking" effect
Application of strong continuous moving distortion effect
Alternating horizontal mirror effect
Horizontal mirror effect and image rotation 90° to the right
Blue-Green overtone effect
Montage of short excerpts in different order
Montage of excerpts of varying duration in different order
Video slowdown (-50%)
Image rotation 20° and zoom (+20%)
Zoom (+200%)
Zoom (+60%)

<b>Test set 4 (extreme or complex alterations)</b>
Application of a sepia effect and light flashes
Application of a strong "shaking" effect
Vignetting effect and opaque mesh overlay 40%
Still image and normal sound
Reverse playback
Zoom (+15%) and opaque mesh overlay 50%
Zoom (+40%) and other reduced content embedded in image (-50%)

The following list summarises the effects tested for music content:

Acceleration of audio signal (+25%)
Acceleration of audio signal (+25%) with change in tone
Acceleration of audio signal (+50%)
Acceleration of audio signal (+50%) with change in tone
Addition of resonance
Addition of strong echo

Addition of light echo
Application of multiple and successive distorting effects
Application of a distorting effect ("secret agent")
Application of a distorting effect ("cartoon")
Deformation of audio signal
Deterioration of audio signal quality
Left-right channel inversion
Slowdown of audio signal (-25%)
Slowdown of audio signal (-25%) with change in tone
Slowdown of audio signal (-50%)
Slowdown of audio signal (-50%) with change in tone
Original signal

## 4. - Matrix of usages observed

The discussions and observation work carried out as part of the mission provide an overview of the current levels of use of the content recognition technologies on the platforms, whether by the platforms themselves in order to enable the blocking of uploaded contents (mainly for audio and video contents) or by rightsholders in order to notify platforms and obtain the removal of unauthorised contents.

The following table summarises these findings, for information purposes only and to the current state of knowledge.

This matrix of uses should not be seen as an exhaustive summary covering all technologies and all existing platforms, as the lack of public and complete information prevents a complete overview to date.

	Music - Audio	Audiovisual	Still images	Editing - DB	Video games
Digital fingerprint recognition	●●●	●●●	●●	●	A
Recognition by <i>hashcode</i>	●●	●●	●●	●	●
Recognition by metadata analysis	●●	●●	●●	●●	●●
Recognition by analysis of digital watermarking	A	A	●●	A	A
<i>Machine learning</i>	A	O	O	A	-
Speech recognition	O	O	-	-	-
Optical character recognition	-	A	A	O	-
Logo or trademark recognition	-	O	O	A	-
Facial or Character Recognition	-	O	O	A	-
Computer vision	-	O	O	-	-

Estimated uses on platforms:

●●●: solution commonly used for the recognition of protected content

●●: solution sometimes used for the recognition of protected content

●: solution rarely used for the recognition of protected content

O: solution used to date but not for the recognition of protected content

A: solution applicable to date but not (or very rarely) used for the recognition of protected content

5. - Provisional and forward-looking information on the possible content of the concepts of “best efforts” and “relevant and necessary information”

<b>Categories of rights</b> on protected works and other objects	<b>Best efforts</b> to be deployed by the platforms <sup>1</sup>	<b>Relevant and necessary information</b> to be provided by rights holders
Rights of audiovisual <b>producers and broadcasters</b>	<b>Video or audio or video and audio fingerprint recognition technology, including over-the-air retransmission (“live content”)</b>	<b>Copy of videograms (producers) and programmes (audiovisual communication companies) with metadata <u>or</u> fingerprints with Metadata</b>
<b>Authors’ copyright on audiovisual works</b> <sup>2</sup>	Video or audio or audio and video fingerprint recognition technology (for already fingerprinted works)	<i>Information on the catalogue of protected rights containing metadata that can be connected back to fingerprints (e.g. ISAN no.)</i>
Rights of <b>phonogram producers</b>	<b>Audio or audio and video fingerprint recognition technology</b>	<b>Copy of records with metadata or fingerprints with metadata</b>
Rights of <b>songwriters and publishers on musical works</b>	Audio <b>fingerprint recognition technology</b> (and, if effective, <b>melody recognition</b> )	<b>Information on the directory of protected rights containing metadata that can be connected back to fingerprints (e.g. ISRC no.)</b>
<b>Publishers</b> of music holding “ <b>graphic exploitation</b> ” rights	Text recognition technology (including on video)	Copying of protected works (texts or scores) with information on the protected rights directory
<b>Copyright</b> on written works ( <b>books</b> )	Text recognition technology or other	Copy of protected works with metadata
<b>Copyright</b> on written works ( <b>press</b> ) and <b>neighbouring rights</b> held by press publishers	Text recognition technology or other	Copies of protected press works and content with metadata
<b>Copyright</b> on <b>visual arts works</b> , including <b>non-moving images</b>	Fingerprint recognition technology	Copies of protected works or fingerprints with <i>metadata</i>
	<u>and/or</u> watermarking recognition technology	Information on digital watermarking affixed and directory of protected rights
<b>Copyright</b> on <b>video games</b>	To be determined	To be determined

**In bold:** techniques deployed by the platforms and information provided today on a significant scale (bold italics if based on isolated agreements)

In non-bold: available techniques that can be used, but have not yet been implemented by the platforms as regards the rights in question.

<sup>1</sup> To be determined in precise detail depending on the presence of works and other protected objects on each platform and the characteristics of each platform

<sup>2</sup> Subject to rights transfer mechanisms



**The concrete scope given to the concepts of “best efforts” and “relevant and necessary information”** referred to in Article 17 of the Directive<sup>73</sup> to define the liability regime applicable to platforms as a result of the provision of unauthorised content will be decisive for the implementation of these provisions, and therefore the rights that they protect. In the field of audio and video content, these concepts will be largely assessed in the light of the performance and functionalities of fingerprinting tools already widely deployed by major platforms, even if other techniques are not excluded in the future (for example, taking into account a digital watermark). With regard to other protected works and objects, **extensive consultation and expertise** is necessary to shed light on the content of these concepts, which may be based on a variety of technologies (digital fingerprints, digital watermarks, character recognition for texts, etc.). The table above, summarising the elements elaborated upon in the report, is intended only to provide a **possible initial perspective** in light of the information gathered by the mission.

**For each sharing service provider, the implications of the notion of “best efforts” is to be determined on a case-by-case basis.** It will depend, for each of the categories of rights concerned, on the content found on the platform and on all the characteristics of the sharing service. It will also depend on the state of the technologies, their efficiency and *“all relevant factors and developments”* (cost, implementation constraints, etc.) while having to be assessed *“in accordance with the industry’s high standards of professional diligence”*.

**For certain content and platforms,** it is possible that *“in certain cases, the availability of unauthorised content protected by copyright can only be avoided by notifying the rightsholders”* (recital 66). At the very least, this would require that the platforms **fully enable right holders to search the content** shared by users based on the descriptions associated with this content.

**Lastly, the concepts of “best efforts” and “relevant and necessary information” are evolving concepts** whose scope must be assessed according to the state of the technologies and uses. They therefore imply regularly updating any assessments made in order to take these factors into account. A complete and operational assessment should go into the detail on the performance and functionalities expected (regarding the “best efforts”) as well as the level of detail or even characteristics and format required (as concerns the “relevant and necessary information”). See for example on the rights management functionalities in the context of digital fingerprinting systems, the possible elements detailed in Appendix 2.

---

<sup>73</sup> In the context of the implementation of Article 17, the liability of the provider of online content-sharing services for the provision of unauthorised content (works and other protected objects) to the public will depend on whether it has provided its *best efforts to ensure the unavailability of specific works and other subject matter for which the rightsholders have provided the service providers with the relevant and necessary information*. Best efforts are defined *“taking into account best practices in the sector and the effectiveness of measures taken in the light of all relevant factors and developments, as well as the principle of proportionality”*.

## 6. - List of persons heard

### **French Ministry of Culture**

#### **Secretariat General**

Alban de Nervaux

Sarah Jacquier

Anne le Morvan

#### **Directorate-General for Media and Cultural Industries (DGMIC)**

Jean-Baptiste Gourdin

#### **Directorate-General for Artistic Creation (DGCA)**

Marion Hislen

Ludovic Julié

Alexandre Therwath

### **European Commission (DG CONNECT)**

Marco Giorello

Camille Auvret

Anneli Andresson

### **Platforms**

#### **Association of Community Internet Services (ASIC)**

Giuseppe de Martino

#### **Dailymotion**

Clément Reix

Etienne Defossez

#### **European Digital Media Association (EDiMA)**

Siada El Ramly

Sebastian Lifflander

Romain Digneaux

### **Facebook**

Anton-Marie Battesti

Béatrice Oeuvarard

### **Google / YouTube**

Benoît Tabaka

David Metge

Thibaut Guiroy

### **Twitch**

Chris Martin

Charlie Slingsby

Gaëlle Lemaire

### **Qwant**

Eric Léandri

Léonard Cox

### **Service providers**

#### **Audible Magic**

Mike Edwards

#### **Blue Effience**

Thierry Chevillard

#### **IMATAG**

Mathieu Desoubeaux

## **INA**

Jean-François Debarnot

Barbara Mutz

Boris Jamet-Fournier

Frédéric Dumas

Jean Carrive

## **LeakiD**

Hervé Lemaire

## **Pex**

Amadea Choplin

## **Ventifier**

Jean-Christophe Le Toquin

## **Webedia**

Antoine Meunier

Julien Bruchet

## **Rightholders**

### **► Visual Arts**

#### **Agence France Presse (AFP)**

Marielle Eudes

Denis Teyssou

Julia Thiébaud

#### **Getty Images**

Jonathan Lookwood

Irene Roberts

**French Society of Authors in the Graphic and Plastic Arts (ADAGP)**

Marie-Anne Ferry-Fall

Thierry Maillard

**French Society of Visual Arts and Fixed Image Authors (SAIF)**

Olivier Brillanceau

Agnès Defaux

**French Society of Authors, Composers and Music Publishers (SACEM)**

David El Sayegh

Thomas Zeggane

Julien Dumon

Héloïse Fontanel

**French Society of Dramatic Authors and Composers (SACD)**

Guillaume Prieur

Hubert Tilliet

Delphine Chassat

**French Civil Society of Multimedia Authors (SCAM)**

Franck Laplanche

Nicolas Mazars

► **Cinema**

**French Association for the Fight against Audiovisual Piracy (ALPA)**

Frédéric Delacroix

Etienne Moron

Clément Hanodin

**United European Independent Distributors (DIRE)**

Hugues QUATTRONE

**French National Federation of Film Publishers (FNEF)**

Hélène Herschel

**French Motion Picture Association (MPA)**

Emilie Anthonis

Okke Delfos Visser

**NBC Universal**

Cordelia Collier

Roz Cochrane-Gough

**French Civil Society of Authors and Producers (ARP)**

Mathieu Debusschère

**French Syndicate of Independent Distributors (SDI)**

Etienne Ollagnier

**French Union of Film Producers (UPC)**

Frédéric Goldsmith

► **Written**

**French National Publishing Union (SNE)**

Julien Chouraqui

**Hachette livre**

Marion Andron

Arnaud Robert

### **Madrigall**

Liliane de Carvalho

### **Relx Group**

Frederic Geraud de Lescauzes

### **► Video games**

#### **Nintendo Europe**

Sebastian Scholl

Neil Boyd

### **► Music**

#### **French Chamber of Trade Unions of Music Publishers (CSEM)/French Chamber of Trade Unions of Music Publishing (CSDEM)**

Carole Guernalec

Yvan Diringer

#### **Believe**

Benoit Lecointe

Benjamin Terray

#### **International Federation of the Phonographic Industry (IFPI)**

Lauri Rechart

Richard Gooch

Patrick Charnley

Elena Blobel

Kristina Janušauskaitė

Lodovico Benvenuti

**Independent Music Companies Association (IMPALA)**

Helen Smith

Matthieu Philibert

**French Civil Society of Phonogram Producers (SCPP)**

Marc Guez

**Civil Society of Phonogram Producers in France (SPPF)**

Karine Colin

**National Association of Phonographic Publishing (SNEP)**

Alexandre Lasch

Emilie Devaux-Trébouvil

**Universal Music**

Sébastien de Gasquet

Jean-Charles Mariani

**Wagram**

Alexis Poncelet

**► Television**

**Canal Plus**

Amélie Meynard

François Mazet

**France Télévisions**

Pierre Linant de Bellefonds

Amel Belkelfa



Dorothee Topin

Adrien Arsenec

### **RMC Découverte**

Guénaëlle Troly

Johanna Chansel

### **TF1**

Anthony Level

### **Users**

#### **La Quadrature du net**

Martin Drago

Arthur Messaud

#### **Guilde des vidéastes**

Guillaume Hidrot

François Theurel

Aude Gogny-Goubert

#### **Videographers**

Ludovic Bassel (Le Tatou)

Mister JD (Jérémy Avril)

Héloïse Wagner (911 Avocats)

### **Other**

#### **CNRS / IRISA**

Laurent Amsaleg